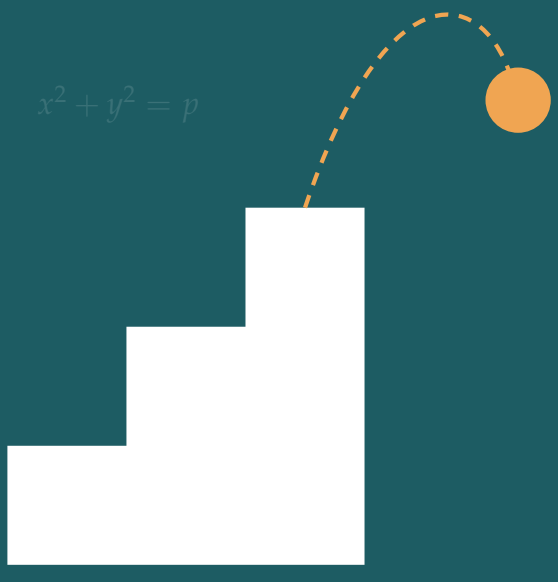
STEP 备试 · 大学数学

Beyond STEP

第 6 章

代数与结构



KEITH McNULTY

Beyond STEP

以历届 STEP 试题为门
走进大学数学

第 6 章

代数与结构

Keith McNulty

Beyond STEP：以历届 STEP 试题为门，走进大学数学

第 6 章：代数与结构

本册是 *Beyond STEP* 全书 13 章中的第 6 章。全书、各章的单行本、每一节的可列印工作纸，以及每一道 STEP 试题的详细解答，均可在 `beyondstep.keithmcnulty.org` 免费阅读及下载。

2026 年 11 月首次于网上发表。

本 PDF 内凡属作者本人创作的内容，包括正文、解答、插图、练习及答案，均按照 Creative Commons CC0 1.0 Universal 授权条款贡献予公有领域：你可以为任何目的复制、改编及分享，毋须征求许可。详见 `creativecommons.org/publicdomain/zero/1.0`。

本书讨论的 STEP 试题，版权属 Cambridge University Press & Assessment 所有。本书并无转载这些试题：每一题均附连结，通往官方来源的题目，即 STEP Support Programme 的试题资料库或 OCR 的历届试卷。

如有错漏，欢迎到 `github.com/keithmcnulty/step_book_mcnulty` 提交 issue 指正。

章

6

代数与结构

代数中每一个巧妙的技巧背后都有一个结构，而理解这个结构，比掌握多少技巧都更有价值。

本章内容

6.1	以单位根为根的多项式	STEP III 2010
6.2	高斯的正十七边形	STEP II 1991
6.3	以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 为根的多项式	STEP II 2023
6.4	解四次方程	STEP III 2017
6.5	从公理出发的微分法	STEP II 1992
6.6	子群的并集	STEP II 1988
6.7	四元数群	STEP III 1993
6.8	由奇异矩阵组成的群	STEP III 1996
A	练习答案	第 59 页

从方程到结构

> 数学是给不同事物起相同名字的艺术。
>
> — 庞加莱（Henri Poincaré）

在历史上的大部分时间里，代数就是解方程。四千年前，巴比伦人已懂得解二次方程；十六世纪的意大利数学家解决了三次和四次方程；其后近三百年间，五次方程却令一切尝试无功而还。到了 1820 至 1830 年代，问题终于有了答案，而这个答案彻底改变了代数。阿贝尔（Niels Henrik Abel）证明了五次方程不存在一般的求根公式，伽罗瓦（Évariste Galois）则确切说明了哪些方程可以求解，他研究的不是方程本身，而是*方程各根的对称性*。为此，他必须创造一种全新的数学对象：群（group）。

从计算答案转向研究结构，这个转变正是本章的主题。现代代数问的不再是“解是甚么?”，而是“这是哪一类对象？它容许哪些运算?”这些问题的答案，既解释了旧有技巧为何奏效，也解决了单靠技巧永远无法解决的问题。

结构为何重要

以下三个古老的问题，两千年来令一切尝试都无功而还：只用直尺和圆规，作出体积为已知立方体两倍的立方体；三等分任意角；作出正 7 边形。三者都不可能做到，而在十九世纪找到的证明，靠的并不是巧妙的作图，而是关于结构的论证：所讨论的是尺规所能到达的数所组成的域（field）的*次数*（degree）（Section 6.3）。同一套理论也解释了为何正 17 边形*可以*作出（Section 6.2），以及为何四次方程可解而五次方程不可解（Section 6.4）。

结构还可以搬到别处去。晶体的对称、多项式各根的置换（permutation）、三维空间的旋转、扭计骰的各种转法，以及椭圆曲线（elliptic curve）上的点，全都满足群的公理（axiom）。只要从公理出发把一条定理证明一次，它便在以上所有情况中成立。这种简约，即庞加莱所说的给“不同事物起相同名字”，正是抽象代数（abstract algebra）如此强大的原因。

你在大学会遇到甚么

在一年级，你会遇到*群*（带有一个运算并满足三条公理的集合），通常还有*环*（ring）和*域*（带有加法和乘法的集合）。你会证明拉格朗日定理（Lagrange's theorem），即子群（subgroup）的大小整除群的大小，并认识置换、对称群（symmetry group）和矩阵群（matrix group）。到了二、三年级，这些内容会引向*伽罗瓦理论*（Galois theory），它把域

和群联系起来，回答有关方程和作图的经典问题；引向表示论（representation theory），它通过矩阵来研究群；还会引向代数数论（algebraic number theory），Section 1.7 中的想法在那里会得到严格的基础。本章最后三节讲的是群。群已不在 STEP 的课程范围之内（已于 2019 年删去），但这些题目本身自成一体，每一节都会给出所需的定义。

贯穿本章的问题

三个大问题

1. **甚么可以由甚么构造出来？**从有理数出发，通过开平方根或解方程，可以到达哪些数？又怎样证明某个数无法到达？
2. **方程的公式为何奏效？**二次、三次和四次方程都有求根公式，背后隐藏的原因是甚么？到了五次，又有甚么改变了？
3. **抽象化带来甚么？**如果我们只凭对象所遵守的规则来描述它们，会有甚么结果？

本章的想法

§	课题	想法
6.1	分圆多项式（cyclotomic polynomials）	按阶（order）把单位根（roots of unity）分类
6.2	正 17 边形	高斯周期（Gauss periods）：和与积给出二次方程
6.3	最小多项式（minimal polynomials）	消去根式；次数相乘
6.4	解四次方程	对称函数（symmetric functions）；三次预解式（resolvent cubic）
6.5	从公理出发的微分法	由规则决定的运算
6.6	子群的并集（union）	从群公理出发作论证
6.7	四元数群（quaternion group）	用矩阵表示运算
6.8	由奇异矩阵（singular matrices）组成的群	按字面理解定义

如何阅读本章

这些题目当中，有不少可以靠蛮力完成：把所有式子展开、比较系数、逐一检查每种情况。如有需要，不妨先这样做。然后回头想一想，是甚么令蛮力行得通，背后有没有结构上的原因。结构上的原因通常较为简短，总是更具启发性，而当蛮力再也行不通时，你需

要的正是它。

6.1 以单位根为根的多项式

题目

STEP III 2010，第 3 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/10-s3-q3`

引子

n 次单位根（roots of unity），即 $z^n = 1$ 的解，位于正 n 边形的各个顶点上。但它们并非全都一样。例如在 12 次单位根之中，1 本身已是一次单位根，-1 是二次单位根，i 是四次单位根，而十二个之中只有四个，即*本原*（primitive）的那些，才需要走足十二步方能回到 1。

按所需的步数把单位根分类，再由每一类构造一个多项式，便得到*分圆多项式*（cyclotomic polynomials，此名源自希腊文，意即“分割圆周”）。它们是 $z^n - 1$ 的基本构件，正如质数是整数的基本构件一样；高斯（Gauss）的正 17 边形作图法（Section 6.2）、单位根筛选法（Section 5.2）以及现代数论中的不少内容，背后都有它们的身影。

动笔之前

想一想 每个 n 次单位根都满足 $z^n = 1$。但使它等于 1 的最小正整数次幂，可能小于 n。对于四个 4 次单位根 1、i、-1、$-\mathrm{i}$，这个最小的幂次分别是多少？

$1^1 = 1$，$(-1)^2 = 1$，而 $\mathrm{i}^4 = (-\mathrm{i})^4 = 1$，且没有更小的幂次可行。所以最小的幂次依次是 1、4、2、4。这个最小的幂次称为该单位根的*阶*（order），而本原 n 次单位根正是阶为 n 的那些单位根。整道题的关键事实是：*每个单位根都恰好有一个阶。*

逐步解题

阶段 1　最初的几个

本原 4 次单位根是 i 和 $-\mathrm{i}$，所以 $C_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1$。 ■

> **想一想**　哪些单位根的阶是 1、2、3、5 和 6？（画出 6 次单位根，并按阶把它们分类。）

阶为 1：只有 1，所以 $C_1(x) = x-1$。阶为 2：只有 -1，所以 $C_2(x) = x+1$。

阶为 3：除 1 以外的三次单位根，即 $\frac{x^3-1}{x-1}$ 的根。所以 $C_3(x) = x^2+x+1$。

阶为 5：除 1 以外的五次单位根，它们是 $\frac{x^5-1}{x-1}$ 的根，所以 $C_5(x) = x^4+x^3+x^2+x+1$。

阶为 6：在六次单位根 $e^{k\pi\mathrm{i}/3}$，$k = 0,\dots,5$ 之中，$k = 0$、3 的阶分别是 1、2，而 $k = 2$、4 的阶是 3。余下的是 $e^{\pm\pi\mathrm{i}/3}$，所以

$$C_6(x) = (x-e^{\mathrm{i}\pi/3})(x-e^{-\mathrm{i}\pi/3}) = x^2 - 2x\cos\tfrac{\pi}{3} + 1 = x^2 - x + 1. \qquad \blacksquare$$

阶段 2　哪个 n 给出 x^4+1？

$x^4+1=0$ 的根满足 $x^4=-1$，所以 $x^8=1$ 但 $x^4\neq 1$。它们的阶整除 8 但不整除 4，所以阶是 8。反过来，阶为 8 的单位根满足 $x^8=1$，$x^4\neq 1$，所以 $x^4=-1$。本原 8 次单位根有四个，x^4+1 的根也有四个，所以 $n=8$。 ■

阶段 3　质数

若 p 是质数，则 p 次单位根的阶整除 p，所以阶是 1 或 p。因此除 1 以外的每个 p 次单位根都是本原的，而

$$C_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+x+1. \qquad \blacksquare$$

阶段 4　没有分圆多项式是另外两个分圆多项式之积

> **停一停，试一试**　假设 $C_q = C_r C_s$。取 C_r 的一个根。它的阶是多少？这条恒等式对它的阶有何说法？由此必然得出甚么？

C_r 的每个根（至少有一个，因为 $e^{2\pi\mathrm{i}/r}$ 是本原的）都是 $C_rC_s = C_q$ 的根，所以它的阶是 q。但它的阶同时也是 r，而一个单位根只有一个阶，所以 $r=q$。于是 $C_q = C_q\,C_s$，又因为 C_q 不是零多项式，所以 $C_s = 1$。这是不可能的，因为 C_s 至少有一个根 $e^{2\pi\mathrm{i}/s}$。所以这样的 q、r、s 并不存在。 ■

回顾

- **按阶分类。**每个单位根都有唯一的阶，按阶分组便把 $z^n - 1$ 的根分成互不相交的类。
- **用根来定义多项式。**每个 C_n 都是借着确切指明哪些数是它的根而确定下来的。
- **唯一性带来不可能性。**第 (iv) 部分只需要一个想法：一个根不可能有两个不同的阶。

背后的数学

分解 $x^n - 1$

每个 n 次单位根都有某个整除 n 的阶 d；而当 $d \mid n$ 时，每个阶为 d 的 d 次单位根都是 n 次单位根。所以 $x^n - 1$ 的根按阶分成若干类，由此得到

$$x^n - 1 = \prod_{d \mid n} C_d(x).$$

例如 $x^6 - 1 = C_1C_2C_3C_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$。图 6.1.1 展示了按这种方式分类的十二个 12 次单位根。本原 n 次单位根的个数，亦即 C_n 的次数，等于 1 至 n 之间与 n 没有公因数的 k 的个数，也就是欧拉函数（Euler's totient function）$\varphi(n)$。比较两边的次数，便得到恒等式 $\sum_{d \mid n} \varphi(d) = n$。

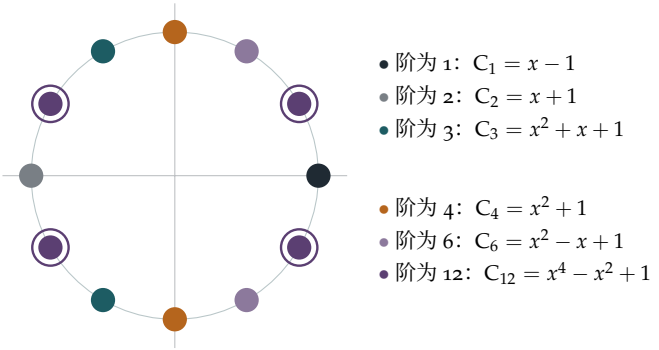


图 6.1.1 十二个 12 次单位根，按阶着色。四个本原 12 次单位根（以圆圈标示）是 C_{12} 的根。各类合起来给出 $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$，次数为 $1+1+2+2+2+4 = 12$。

整数系数，以及一个意外

单看定义并不明显，但每个分圆多项式的系数都是整数。（利用 $x^n - 1$ 的因式分解和归纳法（induction）：C_n 等于 $x^n - 1$ 除以若干个较早的分圆多项式之积，而以首一（monic）整系数多项式对整系数多项式作长除法，所得系数仍是整数。）在很长一段时间里，所有已知例子的系数都只有 0、1 和 -1。第一个例外是 C_{105}，它含有 $-2x^7$ 这一项，由 Migotti 于 1883 年发现；$105 = 3 \times 5 \times 7$ 是具有三个相异奇质因数的最小的数。事实上，分圆多项式的系数可以要多大有多大。

不可约性

第 (iv) 部分证明了没有分圆多项式是另外两个分圆多项式之积。其实更强的结论也成立：C_n 根本不能分解成次数较低的有理系数多项式之积。高斯对 n 为质数的情况证明了这一点（它可由艾森斯坦判别法（Eisenstein's criterion）推出，你会在大学的第一门代数课中遇到），而克罗内克（Kronecker）和戴德金（Dedekind）则证明了一般 n 的情况。正是这种*不可约性*（irreducibility），使分圆多项式成为与单位根有关的多项式之中的“质数”，它也是单位根的伽罗瓦理论（Galois theory）的起点。

思维技巧

先分类，后构造

用一个定义明确的不变量（invariant），把问题中的对象分成若干类，然后逐类建立结构。

这里的不变量是单位根的阶。由于每个根恰好有一个阶，各类互不重叠，于是 $x^n - 1$ 可分解成遍及各类的乘积。同样的模式（由唯一的不变量得出不相交的分解）也是质因数分解和有限阿贝尔群（finite abelian groups）分类的基础。

延伸练习

1. **检查因式分解。**验证 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6 - 1$，并验证 $x^{12} - 1$ 的因式分解如图 6.1.1 所示。
2. **质数的两倍。**证明若 p 是奇质数，则 $C_{2p}(x) = C_p(-x)$。就 $p = 3$ 验证这个结果。
3. **欧拉函数。**证明对于质数 p，有 $\varphi(p^k) = p^k - p^{k-1}$，并且 $C_{p^k}(x) = C_p\left(x^{p^{k-1}}\right)$。利用这个结果求 C_9。

4 较长的一题。 较难利用 $x^{15}-1=\mathrm{C}_1\mathrm{C}_3\mathrm{C}_5\mathrm{C}_{15}$，证明 $\mathrm{C}_{15}(x)=x^8-x^7+x^5-x^4+x^3-x+1$。

延伸阅读

- **Ian Stewart, *Galois Theory***（CRC Press）。大学本科的标准入门书；分圆多项式和正多边形在书中很早便出现。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）。内容包括单位根及其算术性质。
- **Marcus du Sautoy, *Finding Moonshine***（Fourth Estate）。一本讲述对称与群论的科普读物，当中包括伽罗瓦的故事。

6.2 高斯的正十七边形

题目

STEP II 1991，第 4 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/91-s2-q4`

引子

1796 年 3 月 30 日，哥廷根（Göttingen）一名十八岁的学生在他的数学日记写下了第一则记录，这本日记他此后写了一辈子。他发现了怎样用尺规作图（ruler and compasses construction）作出正 17 边形。古希腊人早已懂得作出边数为 3、4、5 和 15 的正多边形（regular polygon），以及边数为这些数目反复加倍的正多边形，但其后两千年间，再没有人添上任何一个新的。高斯（Carl Friedrich Gauss）后来说，正是这项发现令他决心成为数学家，而不是语文学家；相传他还曾要求在自己的墓碑上刻一个正 17 边形。

这个作图法的核心，就是本题的后半部分：四个特定余弦之和等于 $\frac{\sqrt{17}-1}{4}$，这个数只涉及一个平方根。由平方根构成的长度都可以用尺规作出，而高斯再用三个同类的步骤，就能作出 $\cos\frac{2\pi}{17}$ 本身。

动笔之前

? **想一想** 为甚么一道关于正 17 边形的题目，第一部分却是关于 $\cos\frac{2\pi}{5}$ 的?

那是热身，把同一个想法用在较小的多边形上。对正五边形（pentagon）而言，和 $\cos\phi + \cos 2\phi$ 满足一条有理系数的二次方程（quadratic），所以解一条二次方程就能求出它。对正 17 边形而言，四个余弦之和 z 原来也满足一条二次方程。两种情况的窍门都是把余弦相乘，再用 $\cos A\cos B = \frac{1}{2}(\cos(A+B)+\cos(A-B))$ 把乘积变回同一批角的余弦之和。

逐步解题

阶段 1　正五边形

想一想　展开 $y^2=(\cos\phi+\cos 2\phi)^2$，把每个乘积化为和，再利用 $5\phi=2\pi$ 化简 3ϕ 和 4ϕ 这类角。

$y^2=\cos^2\phi+2\cos\phi\cos 2\phi+\cos^2 2\phi=\frac12(1+\cos 2\phi)+(\cos 3\phi+\cos\phi)+\frac12(1+\cos 4\phi)$.

由于 $5\phi=2\pi$，有 $\cos 3\phi=\cos(2\pi-2\phi)=\cos 2\phi$ 和 $\cos 4\phi=\cos\phi$。所以

$$y^2=1+\tfrac12(\cos\phi+\cos 2\phi)+(\cos\phi+\cos 2\phi)=1+\tfrac32 y,$$

即 $2y^2=3y+2$。　■方程 $2y^2-3y-2=(2y+1)(y-2)=0$ 的根是 $y=2$ 和 $y=-\frac12$。但 $y=2$ 需要两个余弦都等于 1，而事实并非如此，所以 $y=-\frac12$。　■

阶段 2　十七次单位根之和为零

$\sum_{k=0}^{16}\cos k\theta$ 是 $\sum_{k=0}^{16}\omega^k$ 的实部(real part),其中 $\omega=e^{\mathrm{i}\theta}$ 是一个 17 次本原单位根(primitive root of unity)。这个等比级数（geometric series）等于 $\frac{\omega^{17}-1}{\omega-1}=0$。　■

所以 $\sum_{k=1}^{16}\cos k\theta=-1$。由于 $\cos(17-k)\theta=\cos k\theta$，各项可以两两配对，于是

$$\sum_{k=1}^{8}\cos k\theta=-\tfrac12.$$

阶段 3　把余弦分成两组

想一想　设 $z=\cos\theta+\cos 2\theta+\cos 4\theta+\cos 8\theta$，并设 z' 为其余四个余弦之和 $\cos 3\theta+\cos 5\theta+\cos 6\theta+\cos 7\theta$。$z+z'$ 是多少?

由第 2 阶段，$z+z'=-\frac12$。如果还能求出 zz'，那么 z 和 z' 就是某条二次方程的两个根。

停一停，试一试　计算 zz'。把它展开成 16 个乘积 $\cos a\theta\cos b\theta$，把每个乘积化为两个余弦之和，然后数一数 $\cos\theta,\cos 2\theta,\dots,\cos 8\theta$ 各出现多少次。（利用 $\cos k\theta=\cos(17-k)\theta$ 和 $\cos(-k\theta)=\cos k\theta$ 化简各角。）

每个乘积给出 $\cos a\theta\cos b\theta=\frac12(\cos(a+b)\theta+\cos(a-b)\theta)$，所以 zz' 是 32 个余弦之和的 $\frac12$ 倍。逐一考虑 $a\in\{1,2,4,8\}$ 和 $b\in\{3,5,6,7\}$ 的 16 对组合：例如 $a=1$、$b=3$ 给出 $\cos 4\theta$ 和 $\cos 2\theta$；$a=8$、$b=7$ 给出 $\cos 15\theta=\cos 2\theta$ 和 $\cos\theta$。对全部十六对都这样

做，$\cos\theta,\ldots,\cos 8\theta$ 每一个都恰好出现四次。因此

$$zz' = \tfrac{1}{2}\times 4\times\sum_{k=1}^{8}\cos k\theta = 2\times\left(-\tfrac{1}{2}\right) = -1.$$

阶段 4 二次方程

所以 z 和 z' 是 $t^2+\frac{1}{2}t-1=0$ 的两个根，即 $4t^2+2t-4=0$，其根为 $t=\frac{-1\pm\sqrt{17}}{4}$。哪一个是 z？按数值计算，$\cos\theta\approx 0.932$、$\cos 2\theta\approx 0.739$、$\cos 4\theta\approx 0.092$ 和 $\cos 8\theta\approx -0.983$，所以 $z\approx 0.78>0$。因此

$$z=\frac{-1+\sqrt{17}}{4}=-\frac{1-\sqrt{17}}{4}.$$ ■

回顾

- **积化和。**余弦的积化和公式把 y^2 和 zz' 变成同一批余弦之和，于是代数运算得以自成一体。
- **和与积给出二次方程。**知道 $z+z'$ 和 zz'，就等于知道以 z 和 z' 为根的二次方程。
- **分组要分得对。**把八个余弦分成 $\{1,2,4,8\}$ 和 $\{3,5,6,7\}$，令每个指标在 zz' 中出现的次数相同。随意分组是行不通的。

背后的数学

高斯周期

为甚么是 $\{1,2,4,8\}$？以 17 为模（modulo），3 的幂 $3^0,3^1,3^2,\ldots$ 会走遍所有非零剩余（residue）：

$$1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6.$$

每隔一个取一个，即 $3^0,3^2,3^4,\ldots$，得出 1、9、13、15、16、8、4、2，以 17 为模就是 ±1、±2、±4、±8：正好是 z 中的角。另一半给出 $\pm3,\pm5,\pm6,\pm7$，即 z' 中的角。高斯把 ω^k 在这类剩余类上的和称为周期（periods）。由于 $17-1=16=2^4$，这些剩余可以对分四次，而在每一阶段，周期都满足一些二次方程，其系数涉及上一阶段的周期。四条二次方程，也就是四个平方根，就从有理数一路通往 $\cos\frac{2\pi}{17}$：

$$\cos\tfrac{2\pi}{17}=\tfrac{1}{16}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\\ +2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\Big).$$

每一步都只涉及平方根，而平方根可以用尺规作出（利用相似三角形或半圆），所以正 17 边形是可作图（constructible）的。

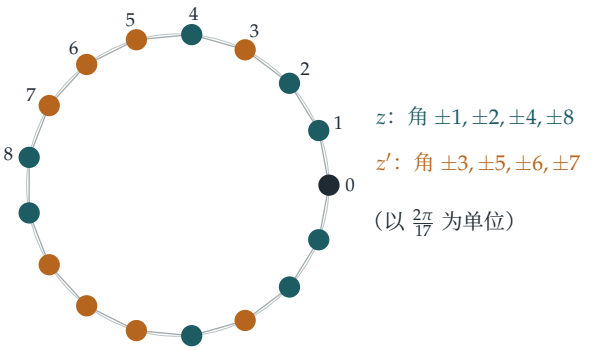


图 6.2.1　正 17 边形的顶点，按高斯的两个周期分成两组。蓝绿色顶点位于角 $\pm 1, \pm 2, \pm 4, \pm 8$（以 $\frac{2\pi}{17}$ 为单位），它们的 x 坐标之和是 $2z = \frac{-1+\sqrt{17}}{2}$；琥珀色顶点则给出 $2z' = \frac{-1-\sqrt{17}}{2}$。

哪些正多边形可以作图？

高斯断言，而 Pierre Wantzel 在 1837 年证明：正 n 边形可以用尺规作出，当且仅当 n 是 2 的幂乘以若干个互不相同的*费马质数*（Fermat primes）之积，费马质数即形如 $2^{2^m}+1$ 的质数。已知的费马质数有 3、5、17、257 和 65537，它们是 Section 1.1 中的费马数。（费马（Fermat）猜想所有这类数都是质数，但欧拉（Euler）证明了 $2^{32}+1$ 可被 641 整除，而此后再没有人找到其他费马质数。）所以正 257 边形和正 65537 边形都可以作图；十九世纪时，Johann Hermes 花了大约十年时间推算出正 65537 边形的作图法，他的手稿现存于哥廷根。正 7 边形和正 11 边形不可作图，因为 7 和 11 不是费马质数（$7-1=6$ 和 $11-1=10$ 都不是 2 的幂）；正 9 边形也不可作图，因为 $9=3^2$ 把费马质数 3 重复了。Wantzel 的证明用到 Section 6.3 中关于域次数（field degrees）的理论。

思维技巧

计算和与积来求出二次方程

要求出一个量，可以为它配上一个自然的伙伴，计算两者的和与积，再解由此得出的二次方程。

个中的艺术在于选对伙伴，使和与积都算得出来。这里的伙伴来自以 17 为模的剩余的对称性，而把这个想法重复四次，就得出高斯的作图法。

延伸练习

1 **正七边形（heptagon）。**试做 STEP II 1995，第 6 题（`step.maths.org/questions/95-s2-q6`）。这道题把高斯将单位根分组的想法用于七次单位根，并求出余弦之和与正弦之和的准确值。判断正弦之和的正负号是当中最微妙的一步。

2 **正五边形。**证明 $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$，并由此描述一个正五边形的尺规作图法。

3 **另一个周期。**用数值验证 $z' = \cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta = \frac{-1-\sqrt{17}}{4}$。

4 **生成元（generators）。**证明以 17 为模时，3 的幂给出所有非零剩余，但 2 的幂却不然。2 的幂给出哪些剩余?

延伸阅读

- **Ian Stewart, *Galois Theory***（CRC Press）。当中有一章讲述尺规作图和正 17 边形。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。第 3 章以浅白优美的笔触介绍作图问题，包括正 17 边形。
- **Daniel Kehlmann, *Measuring the World***（Quercus）。一本关于高斯和洪堡（Alexander von Humboldt）的诙谐小说，可作轻松读物。

6.3 以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 为根的多项式

题目

STEP II 2023，第 4 题

继续阅读之前，请先看题目（原题为英文）。题目载于 OCR 提供下载的 2023 年 STEP 试卷（zip 文件）内的 STEP II 试卷：

`www.ocr.org.uk/Images/707102-2023-past-papers.zip`

引子

$\sqrt{2}$ 是 x^2-2 的根，而这是一个整数系数多项式（polynomial）。同样，$\sqrt{3}$ 是 x^2-3 的根。那么 $\sqrt{2}+\sqrt{3}$ 是否也是某个整数系数多项式的根？$\sqrt{2}+\sqrt{3}+\sqrt{5}$ 又如何？$\sqrt[3]{2}+\sqrt[3]{3}$ 呢？

凡是整数系数多项式的根，都称为*代数数*（algebraic number）。这道题通过亲手消元（elimination），说明代数数之和仍是代数数。计算所得的次数 4、8、6、9 并非偶然：它们量度每个数有多“复杂”，而这种量度，即*域扩张的次数*（degree of a field extension），正是最终解决古希腊倍立方与三等分角问题的关键。

动笔之前

想一想 要找一个以 $\sqrt{2}$ 为根的多项式，你会把 $x=\sqrt{2}$ 平方，从而消去平方根。若有两个不同的平方根，怎样才能逐一消去？

先把其中一个平方根单独移到一边再平方，它便会消失；然后把另一个平方根单独移到一边，再平方一次。每次平方都可能令次数加倍。整道题的策略就是如此：逐一消去根式（radical）。

逐步解题

阶段 1　两个平方根

若 $(x-\sqrt{2})^2=3$，则 $x^2-2\sqrt{2}\,x+2=3$，所以 $x^2-1=2\sqrt{2}\,x$。平方便可消去余下的平方根：$(x^2-1)^2=8x^2$，即

$$x^4-10x^2+1=0. \qquad \blacksquare$$

而 $x=\sqrt{2}+\sqrt{3}$ 满足 $(x-\sqrt{2})^2=(\sqrt{3})^2=3$，所以 $\mathrm{f}(\sqrt{2}+\sqrt{3})=0$。 $\blacksquare$

阶段 2　三个平方根

想一想　设 $x=\sqrt{2}+\sqrt{3}+\sqrt{5}$，则 $x-\sqrt{5}=\sqrt{2}+\sqrt{3}$ 是 f 的根。把 $\mathrm{f}(x-\sqrt{5})=0$ 写成 $P(x)+\sqrt{5}\,Q(x)=0$ 的形式。之后怎样消去 $\sqrt{5}$?

利用 $(x-\sqrt{5})^2=x^2+5-2\sqrt{5}x$ 和 $(x-\sqrt{5})^4=\left(x^2+5-2\sqrt{5}x\right)^2=x^4+30x^2+25-4\sqrt{5}\,x(x^2+5)$ 展开：

$$\mathrm{f}(x-\sqrt{5})=\left(x^4+30x^2+25\right)-4\sqrt{5}\,x(x^2+5)-10\left(x^2+5\right)+20\sqrt{5}\,x+1.$$

合并同类项，得 $P(x)=x^4+20x^2-24$ 和 $Q(x)=-4x^3-20x+20x=-4x^3$。所以 $x^4+20x^2-24=4\sqrt{5}\,x^3$。平方得

$$\left(x^4+20x^2-24\right)^2=80x^6,$$

展开后得

$$\mathrm{g}(x)=x^8-40x^6+352x^4-960x^2+576. \qquad \blacksquare$$

（验算：$(x^4+20x^2-24)^2=x^8+40x^6+352x^4-960x^2+576$，其中用到 $400-48=352$；再减去 $80x^6$ 便得 g。）

阶段 3　一个三次方程与一个平方根

想一想　若 $x=a+\sqrt{2}$，则 $x-\sqrt{2}$ 是 t^3-3t+1 的根。代入后，把含有 $\sqrt{2}$ 的项与不含它的项分开，然后平方。

$(x-\sqrt{2})^3=x^3-3\sqrt{2}\,x^2+6x-2\sqrt{2}$，所以

$$(x-\sqrt{2})^3-3(x-\sqrt{2})+1=\left(x^3+3x+1\right)-\sqrt{2}\left(3x^2-1\right)=0.$$

因此 $(x^3+3x+1)^2=2(3x^2-1)^2$。展开得 $x^6+6x^4+2x^3+9x^2+6x+1=18x^4-12x^2+2$，所以

$$\mathrm{h}(x)=x^6-12x^4+2x^3+21x^2+6x-1. \qquad \blacksquare$$

同样的论证对 $b+\sqrt{2}$ 和 $c+\sqrt{2}$ 也成立，因为我们只用到 a 是 t^3-3t+1 的根这一事实。（h 的另外三个根是 $a-\sqrt{2}$、$b-\sqrt{2}$ 和 $c-\sqrt{2}$，它们是在平方时引入的。）

阶段 4　两个立方根

停一停，试一试 设 $x=\sqrt[3]{2}+\sqrt[3]{3}$。把两边立方。你能否把结果用 x 和单独一个立方根表示?

利用 $(u+v)^3=u^3+v^3+3uv(u+v)$，取 $u=\sqrt[3]{2}$，$v=\sqrt[3]{3}$：

$$x^3=2+3+3\sqrt[3]{6}\,x, \qquad \text{所以} \qquad x^3-5=3\sqrt[3]{6}\,x.$$

再立方一次，便消去最后一个立方根：$(x^3-5)^3=27\cdot 6\,x^3=162x^3$。展开 $(x^3-5)^3=x^9-15x^6+75x^3-125$，得

$$\mathrm{k}(x)=x^9-15x^6-87x^3-125. \qquad \blacksquare$$

回顾

- **逐一消去根式。**把一个根式单独移到一边，取适当的次方，然后重复这个步骤。
- **把有理部分与无理部分分开。**把式子写成 $P+\sqrt{5}\,Q$，再利用 $P^2=5Q^2$，是关键的一步。
- **平方会带来额外的根。**每次平方都会引入“共轭”（conjugate）根，例如除了 $a+\sqrt{2}$ 之外还有 $a-\sqrt{2}$。最后得到的多项式以它们全部为根。

背后的数学

域及其次数

所有形如 $p+q\sqrt{2}$（其中 p、q 为有理数）的数所组成的集合 $\mathbb{Q}(\sqrt{2})$，对加、减、乘、除（除数不为零）都封闭：它是一个域（field）。它是 $\mathbb{Q}$ 上的二维“向量空间”（vector space），以 $1,\sqrt{2}$ 为基底（basis），所以我们说它在 $\mathbb{Q}$ 上的次数（degree）是 2。添加 $\sqrt{3}$ 便得到 $\mathbb{Q}(\sqrt{2},\sqrt{3})$，其基底为 $1,\sqrt{2},\sqrt{3},\sqrt{6}$，次数为 4；再添加 $\sqrt{5}$，次数便是 8（图 6.3.1）。塔定律（tower law）指出，沿着一座域塔往上，次数会相乘。由一个数生成的域，其次数等于该数的最小多项式（minimal polynomial）的次数，即该数所满足的有理系数多项式之中次数最低的一个。可以证明，本题的多项式 f 和 g 都是最小多项式，所以 $\sqrt{2}+\sqrt{3}$ 的次数是 4，而 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 的次数是 8：事实上，单凭 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 这一个数，就足以生成整个 8 次域。

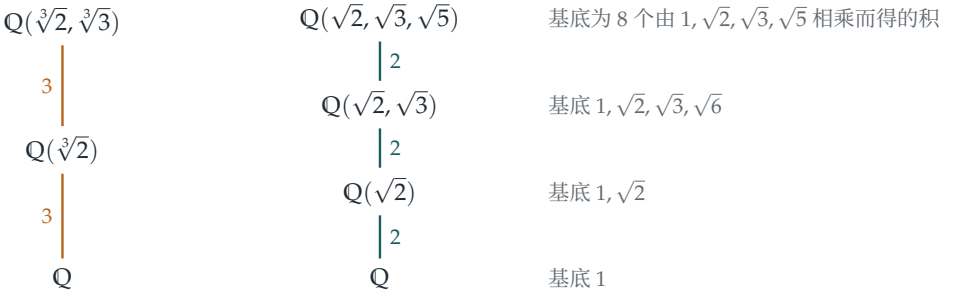


图 6.3.1　域塔。右：每添加一个平方根，次数便加倍，得出 $2\times2\times2=8$，即 g 的次数。左：每添加一个立方根，次数便变为三倍，得出 $3\times3=9$，即 k 的次数。沿着域塔往上，次数会相乘；这条*塔定律*正是证明某些尺规作图不可能完成的关键。

倍立方

尺规作图（ruler-and-compass construction）所能作出的长度，只限于由有理数出发、反复解一次和二次方程而得到的数。每一步都给出一个次数为 1 或 2 的域扩张，所以根据塔定律，每个可作图（constructible）的长度都位于一个次数为 2 的幂的域之内，而它本身的次数也是 2 的幂。但 $\sqrt[3]{2}$ 的最小多项式是 x^3-2，次数为 3。由于 3 不是 2 的幂，$\sqrt[3]{2}$ 不可作图，因此约于公元前 430 年提出的提洛岛（Delos）问题，即用尺规把立方体的体积加倍，是不可能做到的。旺策尔（Pierre Wantzel）在 1837 年证明了这一点，同时证明了一般的角不可能三等分，并完成了可作图正多边形的分类（Section 6.2）。两千年来的种种尝试，就此被一个关于次数的论证画上句号。

代数数构成一个域

本题的方法通过例子说明，代数数之和仍是代数数。一般情况则要用线性代数（linear algebra）来证明：若 α 和 β 的次数分别为 m 和 n，则所有 $\alpha^i\beta^j$（其中 $i<m$，$j<n$）这些数所张成的空间，维数至多为 mn，于是 $mn+1$ 个幂 $1,\alpha+\beta,(\alpha+\beta)^2,\ldots$ 必定线性相关（linearly dependent），由此得出一个次数至多为 mn 的多项式。我们得到的次数 $4=2\times2$、$6=3\times2$ 和 $9=3\times3$ 与这个规律完全吻合。*不是*代数数的数称为*超越数*（transcendental number）；e 和 π 都是例子（分别由埃尔米特（Hermite）于 1873 年及林德曼（Lindemann）于 1882 年证明），而林德曼关于 π 是超越数的定理，也证明了化圆为方同样不可能。

思维技巧

先消去，再量度

要找出一个含根式的式子所满足的多项式，可把根式逐个单独移到一边，再取适当的次方，逐一消去。

然后问一问：次数说明了甚么？最小多项式的次数是该数的一个不变量（invariant），而比较次数是证明某事不可能的最有力方法之一。

延伸练习

1 **本原元（primitive element）。**设 $y=\sqrt{2}+\sqrt{3}$。证明 $y^3=11\sqrt{2}+9\sqrt{3}$，并由此推出 $\sqrt{2}=\frac{1}{2}(y^3-9y)$。因此每个形如 $p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}$ 的数都可以写成 y 的多项式。

2 **混合根式。**求一个次数为 6 的整数系数多项式，使它以 $\sqrt{2}+\sqrt[3]{3}$ 为根。

3 **不可约性（irreducibility）。**证明 x^4-10x^2+1 没有有理根，而且不能写成两个整数系数二次式的积。（提示：试用 $(x^2+ax+b)(x^2-ax+c)$。）由此推出 $\sqrt{2}+\sqrt{3}$ 的次数是 4。

4 **三等分角。**证明 $\cos 3\theta=4\cos^3\theta-3\cos\theta$，并由此推出 $\cos 20^\circ$ 是 $8x^3-6x-1=0$ 的根。假设这个三次方程没有有理根（请自行验证），解释为何不能用尺规把 60° 的角三等分。

延伸阅读

- **Ian Stewart, *Galois Theory***（CRC Press）。讲述域扩张、塔定律及古典作图问题，为大学本科生而写。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。第 3 章证明古希腊几大问题不可能解决，毋须任何预备知识。
- **Robin Hartshorne, *Geometry: Euclid and Beyond***（Springer）。以近世代数处理尺规作图。

6.4 解四次方程

题目

STEP III 2017，第 3 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/17-s3-q3`

引子

每个学生都学过二次方程（quadratic equation）的求根公式。三次方程（cubic）和四次方程（quartic）其实也有公式；这些公式在十六世纪的意大利被发现，其间充满秘密比试，以及为争夺发现权而起的激烈争执。卡尔达诺（Gerolamo Cardano）在 1545 年出版的《大术》（*Ars Magna*）中把两者一并发表：三次方程的解法来自塔尔塔利亚（Niccolò Tartaglia），而塔尔塔利亚曾要他发誓保密；四次方程的解法则来自他自己的学生费拉里（Lodovico Ferrari）。此后近三百年，数学家一直苦苦寻找五次方程（quintic）的公式，却始终徒劳无功。

这道题目展示的，正是解开四次方程的那个窍门，而这个窍门背后大有深意。从四个根出发，按三种可能的方式把根两两配对，得出三个新的量。这三个量满足一个三次方程，而三次方程是你解得到的；有了它们，原来的四个根便随之而来。为甚么这个方法行得通？为甚么四个根可以化约为三个量，五个根却不能如法炮制？正是这个问题，引领伽罗瓦（Galois）创立了群论（group theory）。

动笔之前

想一想 把四件物件 $\alpha, \beta, \gamma, \delta$ 分成两对，共有多少种分法？

三种：$\{\alpha\beta, \gamma\delta\}$、$\{\alpha\gamma, \beta\delta\}$ 和 $\{\alpha\delta, \beta\gamma\}$（图 6.4.1）。题目中的三个量 $\alpha\beta + \gamma\delta$ 等等，正好对应这三种配对。把四个根任意重新排列，只会令这三种配对彼此对调，所以这三个量的任何对称式（symmetric expression），都是四个根的对称式，因而可以用 p、q、r、s 表示。这就是为甚么它们满足一个系数只涉及 p、q、r、s 的三次方程。

逐步解题

阶段 1　欠缺的系数

> **想一想**　在三次方程 $y^3 + Ay^2 + By + C = 0$ 中，根之和用 A 表示是甚么？而 $(\alpha\beta + \gamma\delta) + (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)$ 用四次方程的系数表示又是甚么？

三次方程的根之和是 $-A$。那三个量之和，就是 $\alpha, \beta, \gamma, \delta$ 中两两相乘所得全部六个积之和；对四次多项式 $x^4 + px^3 + qx^2 + rx + s$ 而言，这个和是 q。所以 $A = -q$。

阶段 2　具体的三次方程

代入 $p = 0$、$q = 3$、$r = -6$、$s = 10$，三次方程是

$$y^3 - 3y^2 + (0 - 40)y + (120 - 0 - 36) = y^3 - 3y^2 - 40y + 84 = 0.$$

> **想一想**　试试 84 的细小因数。

$y = 2$ 给出 $8 - 12 - 80 + 84 = 0$。作除法，得 $y^3 - 3y^2 - 40y + 84 = (y - 2)(y^2 - y - 42) = (y - 2)(y - 7)(y + 6)$。最大的根是 7，所以 $\alpha\beta + \gamma\delta = 7$。 ■

阶段 3　根的配对

$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta$，这是全部六个两两之积的和减去 $\alpha\beta + \gamma\delta$，即 $q - 7 = 3 - 7 = -4$。

此外 $\alpha\beta \cdot \gamma\delta = \alpha\beta\gamma\delta = s = 10$。所以 $\alpha\beta$ 和 $\gamma\delta$ 之和为 7，积为 10：它们是 $t^2 - 7t + 10 = (t - 2)(t - 5)$ 的根。由于 $\alpha\beta > \gamma\delta$，得 $\alpha\beta = 5$ 及 $\gamma\delta = 2$。 ■

阶段 4　解四次方程

> **停一停，试一试**　求 $\alpha + \beta$ 和 $\gamma + \delta$。你已知道它们的和（由 p 得出）和它们的积（由第 3 步得出）；要判断哪个是哪个，就用 r。

$\alpha + \beta + \gamma + \delta = -p = 0$ 而 $(\alpha + \beta)(\gamma + \delta) = -4$，所以 $\{\alpha + \beta, \gamma + \delta\} = \{2, -2\}$。系数 r 给出四个三根之积的和：$\alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta = -r = 6$。这可以写成 $\alpha\beta(\gamma + \delta) + \gamma\delta(\alpha + \beta) = 5(\gamma + \delta) + 2(\alpha + \beta)$。若 $\alpha + \beta = 2$，此式等于 $-10 + 4 = -6$；若 $\alpha + \beta = -2$，则等于 $10 - 4 = 6$。所以 $\alpha + \beta = -2$ 及 $\gamma + \delta = 2$。

于是 α、β 是 $t^2 + 2t + 5 = 0$ 的根，即 $-1 \pm 2\mathrm{i}$；而 γ、δ 是 $t^2 - 2t + 2 = 0$ 的根，即 $1 \pm \mathrm{i}$。

四个根是

$$x = -1 \pm 2\mathrm{i}, \qquad x = 1 \pm \mathrm{i}. \qquad \blacksquare$$

验算：$(x^2+2x+5)(x^2-2x+2) = x^4+3x^2-6x+10$。

回顾

- **对称函数（symmetric functions）。**每一步都用上了根与系数的关系：根之和与根之积。
- **降低次数。**一个四次方程的问题变成了一个三次方程（即*预解三次方程*（resolvent cubic）），然后再变成两个二次方程。
- **用尽每一项资料。**p 和 q 给出了各个和与积；s 把 $\alpha\beta$ 和 $\gamma\delta$ 分开；r 则决定了哪一对根配哪一个和。

背后的数学

这个窍门为何行得通：根的置换

1770 年，拉格朗日（Joseph-Louis Lagrange）追问三次和四次方程的解法为何行得通，并在根的*置换*（permutation）中找到了答案。四个根共有 24 种重新排列的方式。在所有这些排列之下，三个量 $y_1 = \alpha\beta + \gamma\delta$、$y_2 = \alpha\gamma + \beta\delta$、$y_3 = \alpha\delta + \beta\gamma$ 只不过是彼此对调：四个根的每一种重新排列，都引致三种配对的一种重新排列（图 6.4.1）。所以它们满足一个 3 次多项式，其系数是各根的对称式。用现代的语言来说，从对称群（symmetric group）S_4（全部 24 个置换）到 S_3（三种配对的 6 个置换）有一个满射的群同态（group homomorphism），这就是四次方程可以化约为三次方程的原因。

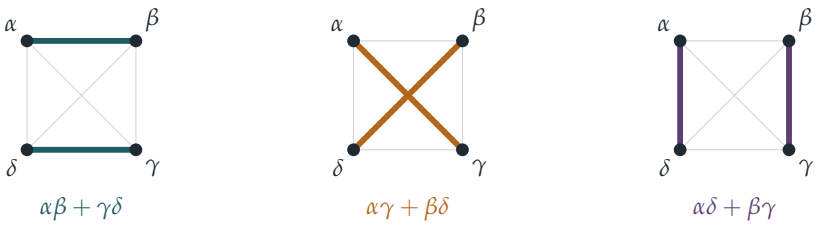


图 6.4.1　把四个根分成两对的三种方式，以及预解三次方程中与之对应的根。$\alpha,\beta,\gamma,\delta$ 的任何重新排列，都只会令这三幅图彼此置换，这就是为甚么那三个量满足一个三次方程，而其系数可以用四次方程的系数表示。

五次方程

对于五个根，拉格朗日尝试寻找一个类似的量，使它在根的置换之下只取寥寥几个值，却找不到有用的。1799 年鲁菲尼（Paolo Ruffini）提出证明，1824 年阿贝尔（Niels Henrik Abel）把证明补全，两人证明了：只用四则运算和根式（radicals），并不存在五次方程的一般求根公式。数年之后，伽罗瓦（Évariste Galois）确切地说明了哪些多项式可以用根式求解：就是那些*根的对称群*能以某种特定方式分解成较简单部分的多项式。对称群 S_4 可以这样分解（经由 S_3 和更小的群），但 S_5 不可以，因为它包含一个大小为 60 的“单”（simple）部分，无法再进一步分解。1832 年，伽罗瓦在决斗中丧生，年仅二十岁；决斗前一晚，他才匆匆把自己的理论写下来。这套理论如今是数学学位课程中的瑰宝之一，通常在三年级学到。

解三次方程

三次方程本身也可以用类似的窍门求解：把一个缺二次项的三次式（depressed cubic）$x^3 - 3px + q$ 写成两个完全立方的组合，从而化约为一个二次方程。这就是练习中那道 2011 年题目所用的方法，它与卡尔达诺公式（Cardano's formula）等价。当三次方程有三个实根时，这条公式在运算途中仍然需要用到复数（complex numbers），正是这个现象迫使数学家认真看待复数（见第 5 章的引言）。

思维技巧

> **对称性化繁为简**
>
> *如果由根构造出来的一些量，在根被置换时只是彼此置换，那么它们满足一个次数较低的多项式，而其系数是你可以计算出来的。*
>
> 这是伽罗瓦理论（Galois theory）的种子：通过理解方程各根的对称性来理解方程本身。

延伸练习

1. **验证三次方程。**验证 $y_1y_2 + y_2y_3 + y_3y_1 = pr - 4s$，其中 $y_1 = \alpha\beta + \gamma\delta$，余类推。（展开并利用 $\sum\alpha = -p$、$\sum\alpha\beta\gamma = -r$、$\alpha\beta\gamma\delta = s$。）

2. **把三次式写成立方之和。**试做 STEP III 2011，第 3 题（`step.maths.org/questions/11-s3-q3`）。这道题把三次式写成两个立方的组合来求解，与本节的路线截然不同。请用数值方法核对它的答案。

3 **另一个四次方程。**用本节的方法解 $x^4 - 4x^3 + 7x^2 - 6x + 2 = 0$。（预解三次方程有一个根是细小的整数。）

4 **数算置换。**在 $\alpha, \beta, \gamma, \delta$ 的 24 个置换中，找出所有把配对 $\{\alpha\beta, \gamma\delta\}$ 变回自身的置换。证明这样的置换共有 8 个。（它们构成 S_4 的一个子群（subgroup）。）

延伸阅读

- **Mario Livio, *The Equation That Couldn't Be Solved***（Simon & Schuster）。五次方程的故事与群论的诞生，适合一般读者。
- **Ian Stewart, *Why Beauty Is Truth: A History of Symmetry***（Basic Books）。从巴比伦人的方程讲到伽罗瓦，再到其后的发展。
- **Ian Stewart, *Galois Theory***（CRC Press）。大学本科教科书，其历史导论所涵盖的正是本节的内容。

6.5 从公理出发的微分法

题目

STEP II 1992，第 4 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/92-s2-q4`

引子

甚么是微分法（differentiation）？在中学，它是用极限（limit）$\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$ 来定义的，然后你再学各种法则：和的导数（derivative）等于导数的和、积法则（product rule），诸如此类。这道题把整件事倒转过来。请把极限完全抛开。假设你对某个运算所知的，就只有它符合和法则、积法则和常数的法则，并且把 x 变成 1。题目要证明的是：这样的运算必定就是微分，至少对多项式（polynomial）而言是如此。

这是代数学家看微积分的角度：一个运算的特征在于它所遵从的法则，而不在于某条公式。遵从积法则的运算称为导子（derivation），它们在代数、几何和物理中随处可见。出人意料的是，训练现代机器学习系统的软件，内里用的也是同一个想法。

动笔之前

想一想 法则 (i) 就是积法则。积法则怎可能告诉你关于常数的任何事情？（试把常数看成一个乘积。）

数 1 等于 1×1。把积法则应用于 1×1，便得出 $\Diamond 1$ 与它自身之间的一个关系，从而迫使它等于零。一般而言，处理这类公理（axiom）的窍门，是把它们应用于精心挑选的简单输入。

逐步解题

阶段 1　常数

想一想　取 $\mathrm{f} = \mathrm{g} = 1$，应用法则 (i)。然后用法则 (iv) 处理其他任何常数。

$\Diamond 1 = \Diamond(1 \cdot 1) = 1 \cdot \Diamond 1 + 1 \cdot \Diamond 1 = 2\Diamond 1$，所以 $\Diamond 1 = 0$。对任意常数 λ，由法则 (iv) 得 $\Diamond \lambda = \Diamond(\lambda \cdot 1) = \lambda \Diamond 1 = 0$。 ■

阶段 2　幂

利用法则 (iii)，$\Diamond x^2 = \Diamond(x \cdot x) = x\Diamond x + x\Diamond x = 2x$。于是

$$\Diamond x^3 = \Diamond(x^2 \cdot x) = x\Diamond x^2 + x^2 \Diamond x = x \cdot 2x + x^2 = 3x^2.$$

停一停，试一试　用归纳法(induction)证明：对每个正整数 n，均有 $\Diamond x^n = n x^{n-1}$。

$n = 1$ 的情况就是法则 (iii)。若 $\Diamond x^n = n x^{n-1}$，则

$$\Diamond x^{n+1} = \Diamond(x^n \cdot x) = x\Diamond x^n + x^n \Diamond x = x \cdot n x^{n-1} + x^n = (n+1)x^n. \qquad \blacksquare$$

阶段 3　所有多项式

一般的多项式是 $\mathrm{h}(x) = a_0 + a_1 x + \cdots + a_m x^m$。由法则 (ii)（重复应用）和法则 (iv)，

$$\begin{aligned} \Diamond \mathrm{h}(x) &= \Diamond a_0 + a_1 \Diamond x + a_2 \Diamond x^2 + \cdots + a_m \Diamond x^m \\ &= a_1 + 2a_2 x + \cdots + m a_m x^{m-1} = \mathrm{h}'(x). \end{aligned} \qquad \blacksquare$$

回顾

- **公理决定运算。**四条法则，完全没有提及极限，就把 $\Diamond$ 在多项式上的作用完全确定下来。
- **生成元（generator）。**每个多项式都是由常数和 x 经加法和乘法构造出来的。只要知道 $\Diamond$ 对这些基本构件的作用，以及它与这些构造运算如何互动，就能确定它在所有多项式上的作用。
- **沿着构造过程作归纳。**证明的步骤紧随多项式的构造方式：先以重复相乘得出幂，然后再求和。

背后的数学

导子

在一个代数系统上，若运算 D 具有可加性（additive），并且满足积法则 $D(fg) = fD(g) + gD(f)$，便称为*导子*。这道题说明，在多项式上，一个把常数变成零的导子完全由 $D(x)$ 决定：事实上 $D(h) = h'(x)\,D(x)$，所以唯一的自由度就是多项式 $D(x)$ 的选择。法则 (iii) 规定了 $D(x) = 1$。导子遍布数学各个领域：在几何中，曲面上的*向量场*（vector field）可以定义为该曲面上的函数的一个导子（它沿着向量场的方向对函数求导）；在代数中，一个结构的导子量度它的“无穷小对称”（infinitesimal symmetries）；在物理中，量子力学的交换子（commutator）$[A, B] = AB - BA$ 对每个变元而言都是一个导子。

没有极限的微积分

在极限完全没有意义的场合，代数式的导数依然行得通。在有限域（finite field）上，例如模质数 p 的算术，并没有极限可言，但多项式的形式导数（formal derivative）仍由同样的法则定义，而且仍然能够侦测重根（repeated root）：多项式 f 有重根，当且仅当 f 与 f' 有公因式。举例说，我们就是这样证明当 $p \nmid n$ 时 $x^n - 1$ 没有重根的；要在有限域上定义 Section 6.1 的分圆多项式（cyclotomic polynomial），就需要这个事实。编码理论和密码学也用到同样的想法。

自动微分

以下是一个现代应用。创造一个数 ε，使得 $\varepsilon^2 = 0$ 但 $\varepsilon \neq 0$，然后用*对偶数*（dual number）$a + b\varepsilon$ 来做算术。这时 $(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon$：$\varepsilon$ 的部分恰好遵从积法则。因此对任何多项式，

$$f(x + \varepsilon) = f(x) + f'(x)\,\varepsilon,$$

而在对偶数 $x + \varepsilon$ 处计算 f，就能同时求出函数值和导数，结果完全准确，既不用极限，也没有因微小差值而产生的舍入误差（图 6.5.1）。这称为*前向模式自动微分*（forward-mode automatic differentiation）。它的近亲“反向模式”（reverse mode），就是用来训练拥有数十亿个参数的神经网络（neural network）的算法（*反向传播*，backpropagation）：这类系统每学习一次，都是在把积法则和链式法则（chain rule）当作导子，一步一步地应用。

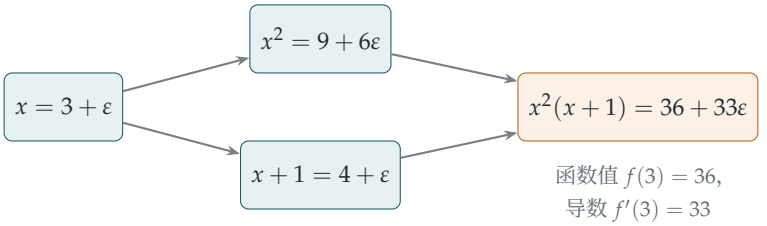


图 6.5.1　用对偶数（$\varepsilon^2 = 0$）对 $f(x) = x^2(x+1)$ 在 $x = 3$ 处作自动微分。每一步都遵从题目中的法则：$(3+\varepsilon)^2 = 9 + 6\varepsilon$，以及 $(9+6\varepsilon)(4+\varepsilon) = 36 + (9+24)\varepsilon$。$\varepsilon$ 的系数就是 $f'(3) = 3\cdot 9 + 2\cdot 3 = 33$，计算结果完全准确。

思维技巧

以性质刻划对象

用一个运算所遵从的法则来描述它，然后证明这些法则唯一地确定了它。

这就是公理化方法（axiomatic method），是大学代数的核心。它的威力在于：凡是由公理证明出来的结果，都适用于每一个满足这些公理的运算，不论那是多项式的微分、曲面上函数的微分，还是某种尚未发明的东西。

延伸练习

1. **另一个导子。**假设 $\Diamond$ 满足法则 (i)、(ii) 和 (iv)，但 $\Diamond x = x$ 而不是 1。证明 $\Diamond \mathrm{h}(x) = x\,\mathrm{h}'(x)$。$\Diamond$ 会把 x^n 变成甚么？

2. **商法则（quotient rule）。**把 $\Diamond$ 推广到有理函数（rational function）f/g，并假设法则 (i) 仍然成立。把法则 (i) 应用于 $\mathrm{g}\cdot\frac{\mathrm{f}}{\mathrm{g}} = \mathrm{f}$，从而推导出商法则。

3. **重根。**证明若 $(x-a)^2$ 整除多项式 f，则 $x-a$ 整除 f′。利用这个结果证明 $x^n - 1$ 没有重根。

4. **对偶数。**设 $f(x) = (x^2+1)^3$，用对偶数计算 $f(2)$ 和 $f'(2)$，并用链式法则验算。

延伸阅读

- **Peter Cameron, *Introduction to Algebra***（Oxford University Press）。大学一年级程度的环、多项式和域，并包括形式导数。

- **Andreas Griewank & Andrea Walther, *Evaluating Derivatives***（SIAM）。自动微分的标准参考书。程度较深。
- **Michael Nielsen, *Neural Networks and Deep Learning***（网上免费阅读）。第 2 章清楚讲解反向传播。

6.6 子群的并集

题目

STEP II 1988，第 9 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/88-s2-q9`

引子

这是全书最短的题目之一，也是最具大学数学特色的题目之一。它谈的是*群*（group），即描述对称的数学语言，问的问题听起来像个谜题：一个群能否被它里面两个较小的群完全覆盖？答案是不能，而证明只有三行。不过三个较小的群却可以做到，这倒是出人意表。

群论（group theory）在 2019 年以前一直属于 STEP 的课程范围，如今则是大学一年级的必修内容。这道题只需要用到定义，下文会一一列出；它正好让你初尝群论学者的思考方式：一个简短而巧妙的论证，除了公理（axiom）之外甚么都不用。

动笔之前

*群*是一个集合 G，连同一个运算（写成乘法 ab），满足：

- 运算符合*结合律*（associative）：$(ab)c = a(bc)$；
- 存在*单位元*（identity）e，对每个 a 都有 $ea = ae = a$；
- 每个 a 都有*逆元*（inverse）a^{-1}，使得 $aa^{-1} = a^{-1}a = e$。

例子：整数（正数、负数和零）在加法下构成群；非零实数在乘法下构成群；正方形的旋转在复合（composition）下构成群。*子群*（subgroup）是 G 的一个子集 K，它在同一运算下本身就是一个群：它包含 e，而且若 $a, b \in K$，则 $ab \in K$ 及 $a^{-1} \in K$。

? **想一想** 若 K 是子群，$a \in K$ 但 $b \notin K$，那么 ab 可以属于 K 吗？

不可以。若 $ab \in K$，则 $b = a^{-1}(ab)$ 是 K 中两个元素的乘积，因而属于 K。这个小小的观察就是整个证明。

逐步解题

阶段 1　两个子群无法覆盖

用反证法（proof by contradiction）：假设 $G = G_1 \cup G_2$，但 G_1 和 G_2 都不是整个 G。

> **想一想**　由于 $G_1 \neq G$，必有一个元素不在 G_1 之中。它必定在哪里？G_2 的情况也一样。现在把这两个元素相乘。

取 $a \in G$ 使得 $a \notin G_1$；由于每个元素都属于 G_1 或 G_2，故 $a \in G_2$。取 $b \in G$ 使得 $b \notin G_2$；于是 $b \in G_1$。考虑乘积 ab。它属于 G_1 或 G_2。

- 若 $ab \in G_1$：由于 $b \in G_1$，$a = (ab)b^{-1} \in G_1$。矛盾。
- 若 $ab \in G_2$：由于 $a \in G_2$，$b = a^{-1}(ab) \in G_2$。矛盾。

无论哪种情况都得出矛盾，所以 $G_1 = G$ 或 $G_2 = G$。 ■

留意我们从未用过 G 是有限群这个条件。这个结果对所有群都成立。

阶段 2　三个子群却可以

> **停一停，试一试**　找出一个群，它是三个子群的并集（union），而这三个子群都不是整个群。（提示：试试一个每个元素都是自己逆元的小群。）

取克莱因四元群（Klein four-group）$V = \{e, a, b, c\}$，其运算规则为 $a^2 = b^2 = c^2 = e$ 以及 $ab = ba = c$、$bc = cb = a$、$ca = ac = b$。（具体来说：一个非正方形的长方形的四个对称，即保持不动、旋转 180°，以及沿两条对称轴之一作反射。又或者是由位元 0、1 组成的数对 (x, y)，在模 2 加法下构成的群。）它的三个子群

$$H_1 = \{e, a\}, \qquad H_2 = \{e, b\}, \qquad H_3 = \{e, c\}$$

各有两个元素，没有一个是整个群，而它们合起来包含了 V 的每一个元素（图 6.6.1）。■

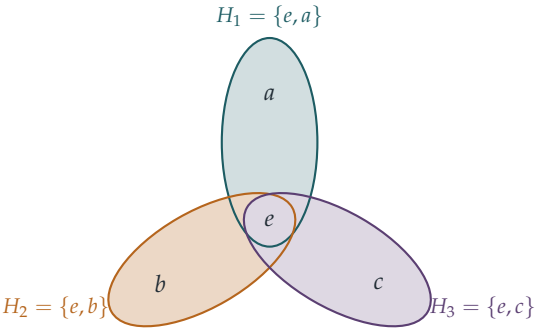


图 6.6.1 克莱因四元群 $\{e, a, b, c\}$ 是它三个 2 阶子群的并集，这三个子群只在单位元 e 处重叠。根据题目的第一部分，没有任何群可以只是两个真子群（proper subgroup）的并集。

回顾

- **选出见证元素，再把它们结合。**证明中在每个子群之外各选一个元素，然后把它们相乘。这种“各取一个再结合”的手法在代数中极为常见。
- **封闭性威力强大。**证明中只用到子群的一个性质：它们在乘法和取逆元之下封闭（closed）。
- **检查你真正需要的假设。**题目给了有限这个条件，却没有用上。察觉到某个假设并非必要，是理解一个证明的一部分。

背后的数学

对称的语言

群在十九世纪同时从几个方向出现：伽罗瓦（Galois）对多项式的根的置换（permutation）的研究（Section 6.4）、柯西（Cauchy）关于置换的工作，以及几何学和晶体学中对对称的研究。上文那个抽象定义，即凡满足三条公理的东西都是群，到该世纪末已经确立。它的威力在于一般性：由公理证明的定理，例如本题中的那一个，同时适用于由数、矩阵、对称和置换构成的各种群。今天群无处不在：在粒子物理学中（标准模型建基于对称群）、在化学中（分子的对称性决定光谱）、在密码学中（椭圆曲线群，Section 1.9），以及在扭计骰（Rubik's cube）的解法之中。

要用多少个子群?

这道题引出一个自然的问题：最少要多少个真子群，它们的并集才是整个群？根据本题，这个数目永远不会是 2。1926 年，Gaetano Scorza 证明了一个群是三个真子群的并集，当且仅当它以克莱因四元群为“商群”（quotient）。1994 年，J. H. E. Cohn 研究了一般的问题，并提出了若干猜想；1997 年，M. J. Tomkinson 证明了没有任何群的这个最小数目是七，尽管由 3 到 6 的每个数都会出现。这类问题叙述简单，却出奇地微妙，正是群论的典型。

向量空间

类似的论证可以证明，实数上的向量空间（vector space）（例如平面或三维空间）永远不可能是有限多个真子空间（proper subspace）的并集：平面不是有限多条通过原点的直线的并集。但在有限域（finite field）上却可以：两个元素的域上的平面，其实又是克莱因四元群，它正是其三条直线的并集。

思维技巧

从公理出发论证

在抽象代数中，你对所处理的对象往往一无所知，只知道它们满足哪些公理。证明必须只用这些公理。

这迫使论证简短而干净利落，就像本题的论证一样，也使它们放诸四海皆准。这需要一些时间去适应，而它正是大学一年级代数课中最独特的体验之一。

延伸练习

1 **验证这个群。**写出克莱因四元群的乘法表，并验证各条群公理。证明它与乘法下的群 $\{1, i, -1, -i\}$ 并不相同。（提示：哪些元素是自己的逆元?）

2 **循环群。**若一个群的每个元素都是某一个元素 g 的幂，则称它为*循环群*（cyclic group）。证明循环群永远不是真子群的并集，不论用多少个。（提示：哪个子群包含 g?）

3 **整数。**直接证明 $(\mathbb{Z}, +)$ 不是子群 $2\mathbb{Z}$（偶数）和 $3\mathbb{Z}$（3 的倍数）的并集。它是否某两个真子群的并集?

4 **平面上的直线。**较难 证明平面 $\mathbb{R}^2$ 不是有限多条通过原点的直线的并集。（提示：每条直线除原点外，最多只包含抛物线 $y = x^2$ 上的一个点。）

延伸阅读

- **M. A. Armstrong, *Groups and Symmetry***（Springer）。一本插图精美的入门教材，以几何例子带动全书。
- **Nathan Carter, *Visual Group Theory***（Mathematical Association of America）。用图像讲解群，最适合在入读大学前阅读。
- **Peter Neumann, Gabrielle Stoy & Edward Thompson, *Groups and Geometry***（Oxford University Press）。牛津大学一年级的经典教材。

6.7 四元数群

题目

STEP III 1993，第 5 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/93-s3-q5`

引子

1843 年 10 月 16 日，哈密顿（William Rowan Hamilton）与妻子沿着都柏林的皇家运河散步时，苦思多年的问题忽然灵光一闪，有了答案。他一直想仿照复数把一对对的数相乘那样，把三个一组的数相乘，却屡试屡败。他突然看出，答案需要的是四个数，而且乘法的次序不可调换：$ij \neq ji$。他把这些法则刻在布鲁穆桥（Brougham Bridge）的石头上：

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1.$$

这就是*四元数*（quaternions）。本题用复数对把四元数构造出来，并在其中找到一个只有八个元素、乘法带点扭曲的小群。时至今日，每一款电脑游戏、每一部飞行模拟器、每一套太空船导航系统，都用四元数来描述三维空间中的旋转。

动笔之前

群的各项定义见 Section 6.6。这里再补充两个用语：群中元素 g 的*阶*（order），是指使 $g^n = e$ 成立的最小正整数 n；若两个群之间存在一个保持运算的一一对应，则称这两个群*同构*（isomorphic），也就是说，它们是“换了标签的同一个群”。

想一想 把数对 (z_1, z_2) 看成代表一个“数” $z_1 + z_2\mathrm{j}$，其中 j 是一个新符号，满足 $\mathrm{j}^2 = -1$，并且对任意复数 w 有 $\mathrm{j}w = w^*\mathrm{j}$。试用这些法则计算 $(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j})$。得出的是否就是 $\circ$ 的公式？

$(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j}) = z_1w_1 + z_1w_2\mathrm{j} + z_2\mathrm{j}w_1 + z_2\mathrm{j}w_2\mathrm{j} = z_1w_1 + z_1w_2\mathrm{j} + z_2w_1^*\mathrm{j} + z_2w_2^*\mathrm{j}^2$，即 $(z_1w_1 - z_2w_2^*) + (z_1w_2 + z_2w_1^*)\mathrm{j}$。答案是肯定的：运算 $\circ$ 其实就是乔装了的四元数乘

法。

逐步解题

阶段 1　借助矩阵证明结合律

直接验证 $(a\circ b)\circ c = a\circ(b\circ c)$，计算十分冗长。其实有更巧妙的方法。

> **想一想**　把 (z_1,z_2) 对应到复矩阵 $M=\begin{pmatrix} z_1 & z_2 \\ -z_2^{*} & z_1^{*}\end{pmatrix}$。矩阵乘积 $M(z_1,z_2)\,M(w_1,w_2)$ 的第一行是甚么？

乘积的第一行是 $(z_1w_1 - z_2w_2^{*},\ z_1w_2 + z_2w_1^{*})$，正好是 $(z_1,z_2)\circ(w_1,w_2)$；第二行是 $(-(z_1w_2 + z_2w_1^{*})^{*},\ (z_1w_1 - z_2w_2^{*})^{*})$，所以乘积仍具有同样的特殊形式。因此 $M(a\circ b) = M(a)M(b)$。矩阵乘法满足结合律（associativity），而 M 是一对一的（从第一行便可读出 z_1、z_2），所以 $\circ$ 满足结合律。 ■

阶段 2　不满足交换律

$(0,1)\circ(\mathrm{i},0) = (0\cdot\mathrm{i} - 1\cdot 0,\ 0\cdot 0 + 1\cdot\mathrm{i}^{*}) = (0,-\mathrm{i})$，但 $(\mathrm{i},0)\circ(0,1) = (0,\mathrm{i})$。所以 $\circ$ 不满足交换律（commutativity）。

四个特殊乘积可由定义直接得出：

$$(z,0)\circ(w,0) = (zw,0),\qquad (z,0)\circ(0,w) = (0,zw),$$
$$(0,z)\circ(w,0) = (0,zw^{*}),\qquad (0,z)\circ(0,w) = (-zw^{*},0).$$

阶段 3　八个元素的群

用四元数的记法，$A=1$，$C=\mathrm{i}$，$B=\mathrm{j}$，$D=\mathrm{ij}=\mathrm{k}$，而 E,G,F,H 则分别是它们的相反数。S_1 的每个元素都具有 $(u,0)$ 或 $(0,u)$ 的形式，其中 $u\in\{1,\mathrm{i},-1,-\mathrm{i}\}$。

> **想一想**　利用四个特殊乘积，证明 S_1 是封闭的。单位元是甚么？

由四个特殊乘积可知，两个形如 $(u,0)$ 或 $(0,u)$ 的元素相乘，结果仍是这两种形式之一，其第一个或第二个分量为 uv、uv^{*} 或 $-uv^{*}$。由于 $\{1,\mathrm{i},-1,-\mathrm{i}\}$ 在乘法、取共轭及取相反数之下都封闭（closed），乘积仍在 S_1 之内。单位元（identity）是 $A=(1,0)$：$(1,0)\circ(w_1,w_2) = (w_1,w_2)$，而且 $(w_1,w_2)\circ(1,0) = (w_1,w_2)$。

> **停一停，试一试**　求出每个元素的阶和逆元。

A 的阶为 1。$E \circ E = (-1,0) \circ (-1,0) = (1,0)$，所以 E 的阶为 2。对于 $C = (\mathrm{i},0)$：$C \circ C = (-1,0) = E$，所以 C 的阶为 4，而 $C^{-1} = C^3 = E \circ C = G$。对于 $B = (0,1)$：$B \circ B = (-1 \cdot 1^*, 0) = (-1,0) = E$，所以 B 的阶为 4，而 $B^{-1} = F$。同理，$D \circ D = (-\mathrm{i} \cdot \mathrm{i}^*, 0) = (-\mathrm{i} \cdot (-\mathrm{i}), 0) = (-1,0) = E$，所以 D 的阶为 4，逆元（inverse）为 H。至于 G、F、H，它们分别是 C、B、D 的逆元，阶同样为 4。总结如下：

元素	A	B	C	D	E	F	G	H
逆元	A	F	G	H	E	B	C	D
阶	1	4	4	4	2	4	4	4

既有封闭性和结合律（第 1 步），又有单位元和逆元，S_1 是一个群。■这个群称为*四元数群*（quaternion group）Q_8。

阶段 4 一个子群

$\{A, B, E, F\} = \{1, \mathrm{j}, -1, -\mathrm{j}\}$ 由 B 的各次幂组成：$B^1 = B$，$B^2 = E$，$B^3 = F$，$B^4 = A$。所以它是封闭的，并且包含各元素的逆元：这是一个子群（subgroup），而且是阶为 4 的*循环群*（cyclic group）。矩阵 $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 满足 $J^2 = -I$，$J^3 = -J$，$J^4 = I$，所以它同样生成一个阶为 4 的循环群。对应 $B^k \leftrightarrow J^k$ 是一个同构。■（事实上，J 正是 $M(0,1)$，即 B 所对应的矩阵。）

回顾

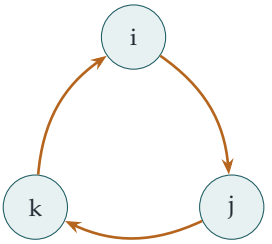
- **用矩阵来表示。**结合律直接验证起来十分费劲，这里却可从矩阵乘法继承过来。
- **找出公式背后的结构。**古怪的运算 $\circ$ 原来就是四元数乘法，看穿了这一点，一切都变得容易。
- **阶和逆元刻划了一个群。**单看各元素的阶，已可见 Q_8 与别不同：一个阶为 2 的元素，六个阶为 4 的元素。

背后的数学

复数之外

实数构成一个一维的数系，在其中可以做加法、乘法和除法；复数则构成一个二维的数系。哈密顿的四元数是四维的，除法依然可行，但乘法不再满足交换律（图 6.7.1）。1878 年，弗罗贝尼乌斯（Ferdinand Frobenius）证明了 $\mathbb{R}$、$\mathbb{C}$ 和 $\mathbb{H}$（取自 Hamilton 的首

字母）这三者，是实数域上仅有的、乘法满足结合律的有限维“可除代数”（division algebras）。如果放弃结合律，但保留一个可乘的大小，即 $|xy| = |x|\,|y|$，一如实数、复数和四元数那样，那就恰好还多一个：八维的八元数（octonions），由 John Graves 和凯莱（Arthur Cayley）在 1840 年代发现。赫维兹（Adolf Hurwitz）于 1898 年证明，这类数系就只有这四个。（若不设关于大小的条件，还有其他更古怪的非结合可除代数，但 1958 年一条由博特（Raoul Bott）、米尔诺（John Milnor）和 Michel Kervaire 得出的深刻定理指出，任何有限维实可除代数的维数必为 1、2、4 或 8。）



顺着箭头：$\mathrm{ij} = \mathrm{k}$，$\mathrm{jk} = \mathrm{i}$，$\mathrm{ki} = \mathrm{j}$

逆着箭头：$\mathrm{ji} = -\mathrm{k}$，$\mathrm{kj} = -\mathrm{i}$，$\mathrm{ik} = -\mathrm{j}$

以及 $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$

图 6.7.1　哈密顿的乘法法则。把 i、j、k 其中两个顺着箭头方向相乘，得到第三个；逆着箭头方向相乘，则得到第三个的相反数。$\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}$ 这八个元素构成本题的四元数群 Q_8。

三维空间中的旋转

模（modulus）为 1 的四元数描述三维空间的旋转：绕单位轴 $\mathbf{u}$ 转过角度 θ 的旋转，对应于 $q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}(u_1\mathrm{i} + u_2\mathrm{j} + u_3\mathrm{k})$，它作用于向量 $\mathbf{v}$（写成 $v_1\mathrm{i} + v_2\mathrm{j} + v_3\mathrm{k}$）的方式是 $\mathbf{v} \mapsto q\mathbf{v}q^{-1}$。旋转的复合就是四元数的相乘。这比使用矩阵或角度更有效率，数值上也更稳定，而且避开了“万向节锁”（gimbal lock）：那是失去一个自由度的现象，当年阿波罗（Apollo）太空人使用以陀螺仪为本的导航系统时，就不得不设法绕过这个问题。半角 $\frac{\theta}{2}$ 也透露出一点深刻的端倪：旋转 360° 得到的是 $q = -1$，而不是 1，物理学家在电子的行为（自旋，spin）中正好看到这个事实。

四平方和

四元数的模是可乘的，$|pq| = |p||q|$，与复数的模一样。把它展开写出，便得到欧拉（Euler）的*四平方恒等式*（four-square identity）：两个四平方和之积，本身也是一个四平方和。这正是拉格朗日（Lagrange）定理的关键一步，该定理指出每个正整数都是四个平方数之和；我们会在 Section 7.8 证明这条定理，它是 Section 1.6 中二平方和结果的四维近亲。

思维技巧

把抽象的对象具体地表示出来

如果一个抽象的运算难以推理，就找一个具体的模型（例如矩阵），让它在其中变成熟悉的运算。

这样，结合律之类的性质便不费吹灰之力。这个想法，即把群表示为矩阵来研究，后来发展成一门庞大而优美的学科：*表示论*（representation theory）。

延伸练习

1 **哈密顿的法则。**利用数对，验证 $C \circ B = D$ 及 $B \circ C = H$，即 $\mathrm{ij} = \mathrm{k}$ 及 $\mathrm{ji} = -\mathrm{k}$。

2 **只有一个阶为 2 的元素。**证明 $E = -1$ 是 Q_8 中唯一阶为 2 的元素。由此推断 Q_8 与正方形的对称群（它有五个阶为 2 的元素）并不同构。

3 **四平方和。**证明 $\det M(z_1, z_2) = |z_1|^2 + |z_2|^2$。利用 $\det(M_1 M_2) = \det M_1 \det M_2$，推断两个四平方和之积是一个四平方和。

4 **子群。**找出 Q_8 的所有子群。证明除了 $\{A\}$ 之外，每个子群都包含 E，并证明 Q_8 是它三个阶为 4 的循环子群的并集（试与 Section 6.6 比较）。

延伸阅读

- **John Conway & Derek Smith, *On Quaternions and Octonions***（A. K. Peters）。讲述四元数和八元数的几何与算术。程度较深，但引人入胜。
- **John Baez, "The octonions"**，*Bulletin of the American Mathematical Society* 39 (2002)；网上亦可免费阅览。一篇精彩的综述；引言部分现在就读得懂。
- **Andrew Hanson, *Visualizing Quaternions***（Morgan Kaufmann）。讲述以四元数处理旋转，并介绍其在电脑图像方面的应用。

6.8 由奇异矩阵组成的群

题目

STEP III 1996，第 6 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

`step.maths.org/questions/96-s3-q6`

引子

每个学生都学过：行列式（determinant）为零的矩阵没有逆矩阵。那么，一个由矩阵组成的群（group），既然其中每个元素都有逆元（inverse），就肯定不可能包含任何奇异矩阵（singular matrix）吧?

其实可以。关键在于“逆”这个字。在群里，$\mathbf{A}$ 的逆元是指与 $\mathbf{A}$ 结合后得出*该群的*单位元（identity element）的那个元素，而没有任何规定说群的单位元必须是单位矩阵（identity matrix）$\mathbf{I}$。本题构造出一个群，其中每个矩阵都是奇异的，而单位元本身就是一个行列式为零的矩阵。这一课教我们要按字面去读定义，也教我们分清抽象结构与我们最初认识它时所见的那个熟悉例子。

动笔之前

群的定义见 Section 6.6。

想一想 在第 (i) 部分，单位矩阵 $\mathbf{I}$ 并不是 $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ 这种形式。那么 S 的单位元会是甚么?

它必须是 S 中的某个矩阵 $\mathbf{E}$，使得对 S 中每个 $\mathbf{X}$ 都有 $\mathbf{EX} = \mathbf{XE} = \mathbf{X}$。这个条件只涉及 $\mathbf{E}$ 怎样作用于这种特殊形式的矩阵，而不是所有矩阵。解方程就可以把它找出来。

逐步解题

阶段 1　封闭性（closure）

以 $\mathbf{M}_a$ 表示四个项全都等于 a 的矩阵。那么

$$\mathbf{M}_a\mathbf{M}_b = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} = \mathbf{M}_{2ab},$$

而当 $a, b \neq 0$ 时，$2ab \neq 0$。所以 S 是封闭的。 ■

阶段 2　群公理（group axioms）

> **想一想**　矩阵乘法满足结合律。至于单位元，解 $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_a$。至于逆元，解 $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_e$。

结合律（*associativity*）由矩阵乘法继承而来。单位元：$\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_{2ea} = \mathbf{M}_a$ 对所有 a 成立，当且仅当 $e = \frac{1}{2}$；由于公式是对称的，$\mathbf{M}_a\mathbf{M}_{1/2} = \mathbf{M}_a$ 同样成立。所以

$$\mathbf{E} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

是 S 的单位元。逆元：当 $b = \frac{1}{4a}$ 时，$\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab} = \mathbf{M}_{1/2}$，而这个值不为零，所以 $\mathbf{M}_{1/(4a)}$ 是 $\mathbf{M}_a$ 在 S 中的逆元。因此 S 是一个群。 ■每个元素的行列式都是 $a^2 - a^2 = 0$。

阶段 3　奇异性会蔓延

> **停一停，试一试**　假设 $\mathbf{A} \in G$ 是奇异的，并设 $\mathbf{B}$ 为 G 的任意元素。把 $\mathbf{B}$ 写成一个含有 $\mathbf{A}$ 的乘积，然后取行列式。

以 $\mathbf{A}^{-1}$ 表示 $\mathbf{A}$ 在群 G 中的逆元（不一定是逆矩阵）。那么 $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$ 属于 G，而且

$$\mathbf{AC} = \mathbf{A}\mathbf{A}^{-1}\mathbf{B} = \mathbf{EB} = \mathbf{B}.$$

取行列式，得 $\det\mathbf{B} = \det\mathbf{A}\,\det\mathbf{C} = 0$。所以 G 的每个元素都是奇异的。 ■特别地，如果一个矩阵群中有一个元素作为矩阵是可逆（invertible）的，那么所有元素都可逆；一个矩阵群要么全部可逆，要么全部奇异。

阶段 4　一个 3×3 的例子

想一想 你能把第 (i) 部分推广到 3×3 矩阵吗？或者找一个更简单的例子，用一个“无视”三个坐标中其中两个的矩阵？

取

$$G = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : a \neq 0 \right\}.$$

角上的项分别为 a 和 b 的两个矩阵，乘积就是角上的项为 ab 的矩阵，所以 G 是封闭的；乘法满足结合律；单位元是角上的项为 1 的矩阵；角上的项为 a 的矩阵，其逆元是角上的项为 $\frac{1}{a}$ 的矩阵。所以 G 是一个群，而且每个元素的行列式都是 0。 ■（另一个例子：九个项全都等于 $a \neq 0$ 的 3×3 矩阵，其单位元的所有项都是 $\frac{1}{3}$。）

回顾

- **按字面去读定义。**群的单位元就是*在该群之内起单位元作用的那个元素*；它不一定是我们熟悉的那个单位矩阵。
- **解方程求出结构。**S 的单位元和逆元都是靠解方程找出来的，而不是靠猜。
- **行列式具有可乘性。**单凭这一个性质，就说明了奇异性会由一个元素蔓延到所有元素。

背后的数学

幂等元与隐藏的可逆性

任何矩阵群的单位元 $\mathbf{E}$ 都满足 $\mathbf{E}^2 = \mathbf{E}$：它是*幂等*（*idempotent*）的。从几何上看，幂等矩阵就是一个*投影*（*projection*）：它把每个向量映射到某个子空间（subspace）上，而原本已在该子空间内的向量则保持不变。在第 (i) 部分，$\mathbf{E}$ 把平面投影到直线 $y = x$ 上，而每个矩阵 $\mathbf{M}_a$ 都是先投影到这条直线上，然后沿着它以因子 $2a$ 拉伸（图 6.8.1）。在这条直线上，这个群的作用是可逆的拉伸；它只是无视了与直线垂直的方向。所以 S 其实就是非零实数的乘法群（通过 $\mathbf{M}_a \mapsto 2a$），只不过它栖身于平面内的一条直线上。这个结论普遍成立：每个由矩阵组成的群，经过换基（change of basis）之后，都是一个由可逆矩阵组成的群，作用于其单位元的像上，其余位置则以零填充。

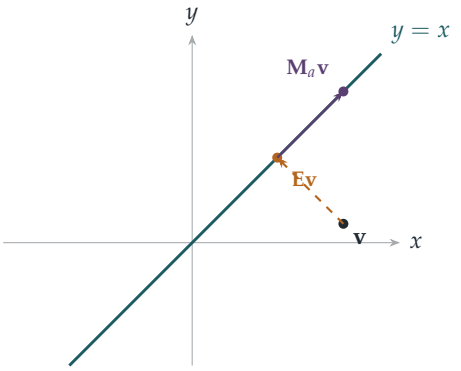


图 6.8.1　第 (i) 部分的矩阵所起的作用。单位元 $\mathbf{E}$ 把每个向量 $\mathbf{v}$ 投影到直线 $y = x$ 上（琥珀色虚线）。每个 $\mathbf{M}_a$ 都先作同样的投影，然后沿着直线以因子 $2a$ 拉伸（紫红色；图中 $2a = \frac{16}{9}$）。在这条直线本身之上，这个群的作用就是普通的可逆缩放。

抽象与具体

人们最早研究的群都是具体的：置换（permutation）、对称、可逆矩阵。抽象的定义（一个集合连同一个满足三条公理的运算）是从这些例子中提炼出来的。本题显示了抽象观点的价值：S 与非零实数的乘法群是*同构*（*isomorphic*）的，即同一个群换了一身衣服，尽管一个由奇异矩阵组成，另一个由数组成。辨认出两个外表不同的结构何时“相同”，是代数最核心的技巧之一，而数学家正是藉同构这个概念把这种“相同”说得精确。

思维技巧

质疑对熟悉对象的隐藏假设

当一个熟悉的对象出现在抽象定义中时，要查清楚定义实际上要求它具备哪些我们熟悉的性质。

“矩阵群的单位元是 $\mathbf{I}$”听起来理所当然，却不是定义的一部分；放下这个假设，就得出了一个真正崭新的例子。许多新的数学结构，正是这样靠质疑假设而发现的。

延伸练习

1 **一个同构。**证明映射 $\mathbf{M}_a \mapsto 2a$ 是由 S 到非零实数的一一对应（one-to-one correspondence），并且把矩阵乘法变成数的乘法。

2 **不是群。**证明所有形如 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 且 $a \neq 0$ 的矩阵所组成的集合在乘法下封闭，但不是一个群。（提示：试找单位元。有没有左单位元？有没有右单位元?）

3 **幂等元。**求所有满足 $\mathbf{E}^2 = \mathbf{E}$ 的 2×2 实矩阵 $\mathbf{E}$，并从几何角度描述它们。

4 **所有项相等。**证明所有项都等于 $a \neq 0$ 的 $n \times n$ 矩阵在乘法下构成一个群，并求它的单位元。

延伸阅读

- **M. A. Armstrong, *Groups and Symmetry***（Springer）。讲述矩阵群与同构，并附有大量几何例子。
- **Gilbert Strang, *Introduction to Linear Algebra***（Wellesley-Cambridge）。对投影与幂等矩阵有清晰的讲解。
- **Joseph Gallian, *Contemporary Abstract Algebra***（CRC Press）。一本平易近人的入门教材，载有许多不寻常的群的例子。

我们学到了甚么

本章开首，我们谈到代数的重心由解方程转移到研究结构，并提出了三个问题：甚么可以由甚么构造出来？方程的公式为何行得通？抽象化带来了甚么好处？以下是本章八道题目所揭示的答案。

1. 甚么可以由甚么构造出来？

在 Section 6.3 中，我们逐一消去根式（radical），找出 $\sqrt{2}+\sqrt{3}$、$\sqrt{2}+\sqrt{3}+\sqrt{5}$ 和 $\sqrt[3]{2}+\sqrt[3]{3}$ 所满足的多项式，次数分别为 4、8 和 9。这些次数是不变量（invariant）：它们就是该数所生成的域（field）的次数。由于次数沿着域塔（tower of fields）逐层相乘，凡是可以用平方根得到的数，其次数必为 2 的幂。单凭这一点，便足以证明倍立方不可能做到（$\sqrt[3]{2}$ 的次数是 3），也证明 60° 角不可能三等分。

反过来，Section 6.2 展示了某些东西可以怎样构造出来。把 17 次单位根（roots of unity）分拆成高斯（Gauss）周期（period）之后，和 $\cos\frac{2\pi}{17}+\cos\frac{4\pi}{17}+\cos\frac{8\pi}{17}+\cos\frac{16\pi}{17}$ 满足一个二次方程，其根为 $\frac{-1+\sqrt{17}}{4}$；再解三个二次方程便可得到 $\cos\frac{2\pi}{17}$，从而作出正 17 边形。这两节的背后，都是 Section 6.1 的分圆多项式（cyclotomic polynomial）：它们是 x^n-1 的基本构件，把单位根按阶（order）分类便可得到。

2. 方程的公式为何行得通？

Section 6.4 揭示了四次方程（quartic）的秘密：由四个根组成三个量 $\alpha\beta+\gamma\delta$、$\alpha\gamma+\beta\delta$、$\alpha\delta+\beta\gamma$，每个量对应把四个根两两配对的一种方法。无论怎样重新排列这些根，都只会把这三个量互相调换，所以它们满足一个系数已知的三次方程。先解这个三次方程，再解两个二次方程，便得出四个根。拉格朗日（Lagrange）看出，这个方法之所以行得通，在于四个物件的置换（permutation）如何作用于那三种配对；伽罗瓦（Galois）则看出，这个方法对五个根失效，是因为五个物件的置换群（group）之中，有一部分无法再分解。这些公式，其实是群结构的影子。

3. 抽象化带来了甚么好处？

最后四节都以物件所遵守的规则来描述物件。

- 在 Section 6.5 中，四条规则（可加性、乘积法则、常数、$\Diamond x=1$）迫使一个运算必然是求导（differentiation），完全不涉及极限。同样的规则，正是现代软件中自动微分

（automatic differentiation）的基础。

- 在 Section 6.6 中，由群公理（axiom）出发的一个三行论证，一举对所有群证明了：没有任何群是两个真子群（proper subgroup）的并集。
- 在 Section 6.7 中，一个定义在复数对上的古怪运算，原来就是哈密顿（Hamilton）的四元数（quaternion）乘法；用矩阵来表示它，结合律（associativity）便自动成立。
- 在 Section 6.8 中，按字面理解群的定义，便得出一个由奇异矩阵（singular matrix）组成的群，它的单位元（identity）并不是单位矩阵，而它“其实”是非零实数群的化身。

在每一个例子中，抽象的观点都解释了一些单靠计算会被掩盖的东西。

4. 代数工具箱

方法	在哪里用过
按唯一的不变量分类	按阶把单位根分类（6.1）
由和与积得出二次方程	高斯周期（6.2）；四次方程（6.4）
积化和差公式	正 17 边形（6.2）
消去根式	最小多项式（minimal polynomial）（6.3）
次数与塔定律（tower law）	作图的不可能性（6.3）
根的对称函数（symmetric function）	三次预解式（resolvent cubic）（6.4）
由公理确定一个运算	导子（derivation）（6.5）
由群公理出发论证	子群的并集（6.6）
矩阵表示（matrix representation）	四元数（6.7）
同构（isomorphism）	奇异矩阵群（6.8）

下一步

- 四元数通往 Section 7.8 的拉格朗日四平方和定理（four-square theorem）。
- 把矩阵视为自有一套规则的代数物件，是第 7 章的主题。
- 像高斯整数（Gaussian integers）这类数系的算术，当中因数分解（factorisation）可能失效，是 Section 1.7 的主题。

如果你想在上大学之前再走远一点

- **Mario Livio, *The Equation That Couldn't Be Solved***：五次方程、伽罗瓦与群论的诞生。
- **Nathan Carter, *Visual Group Theory***：用图像认识群，是初次接触的理想读物。

- **M. A. Armstrong, *Groups and Symmetry***：建基于几何的大学入门课程。
- **Ian Stewart, *Galois Theory***：留待你准备好了解整个故事的时候。

伽罗瓦在一场决斗之后去世，年仅二十岁，只留下数十页手稿，数学界花了几十年才读懂。他看出，一个方程最深层的秘密并不在它的系数之中，而在它的解的对称性之中。这个洞见——给不同的东西起同一个名字，并研究它们共有的结构——如今贯穿整个数学。你已经在多项式、多边形、四元数和矩阵中见过它发挥作用；到了大学，你几乎处处都会遇见它。

延伸练习答案

以下只是简短的答案和提示，并非完整解答：这里只列出结果和关键步骤，方便你核对自己的做法。请先认真做过每一道练习，然后才看答案。

6.1 以单位根为根的多项式

1. $(x-1)(x+1) = x^2-1$ 而 $(x^2+x+1)(x^2-x+1) = x^4+x^2+1$，两者之积为 x^6-1。同理，$x^{12}-1 = (x^6-1)(x^6+1)$，而 $x^6+1 = (x^2+1)(x^4-x^2+1) = \mathrm{C}_4\mathrm{C}_{12}$。

2. $2p$ 的因数（divisor）为 1、2、p、$2p$，所以 $\mathrm{C}_{2p} = \frac{x^{2p}-1}{(x-1)(x+1)\mathrm{C}_p(x)} = \frac{x^p+1}{x+1}$。另一方面，$\mathrm{C}_p(-x) = \frac{(-x)^p-1}{-x-1} = \frac{x^p+1}{x+1}$，因为 p 是奇数。当 $p=3$ 时：$\mathrm{C}_6 = x^2-x+1 = \mathrm{C}_3(-x)$。

3. 不超过 p^k 而又与 p^k 有公因数的数，就是那 p^{k-1} 个 p 的倍数。本原（primitive）p^k 次单位根是 $x^{p^k}-1$ 的根之中不属于 $x^{p^{k-1}}-1$ 的根的那些，所以 $\mathrm{C}_{p^k} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = \mathrm{C}_p\left(x^{p^{k-1}}\right)$。因此 $\mathrm{C}_9 = x^6+x^3+1$。

4. $\mathrm{C}_{15} = \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$。把 $(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)$ 与题中给出的八次式相乘并展开，验证结果为 $x^{15}-1$。

6.2 高斯的正十七边形

1. $\eta+\eta'$ 是全部六个非实七次单位根之和，即 -1。展开 $\eta\eta'$ 得到九项 α^{a+b}，其指数为 $4,6,0,5,0,1,0,2,3$（模 7）：即三个 1，以及每个非实根各出现一次，所以 $\eta\eta' = 3-1 = 2$。因此 η、η' 就是 $\frac{-1\pm\mathrm{i}\sqrt{7}}{2}$。$\eta$ 的实部给出余弦之和。它的虚部是 $\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7}$，由于 $\sin\frac{4\pi}{7} = \sin\frac{3\pi}{7} > \sin\frac{\pi}{7}$，这个值为正；所以它等于 $+\frac{\sqrt{7}}{2}$。

2. 设 $\zeta = \mathrm{e}^{2\pi\mathrm{i}/5}$，则两个周期（period）$\zeta+\zeta^4 = 2\cos\frac{2\pi}{5}$ 和 $\zeta^2+\zeta^3$ 之和为 -1，之积为 -1，所以它们是 $t^2+t-1=0$ 的根，而其中的正根给出 $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$。作图方法：在单位圆内，两条直角边为 1 和 $\frac{1}{2}$ 的直角三角形，斜边长为 $\frac{\sqrt{5}}{2}$；减去 $\frac{1}{2}$ 再取一半，便得 $\cos\frac{2\pi}{5}$。在轴上这个距离处作垂线，它与圆相交于一个与 $(1,0)$ 相邻的顶点；再用这条弦沿圆周逐步截取。

3. 两者准确至小数点后五位都是 -1.28078。

4. 3 的各次幂依次为 $3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,1$：十六个数全部出现。2 的各次幂在八步之后重复（$2^8 = 256 \equiv 1$），给出 $\{1,2,4,8,9,13,15,16\}$，即模 17 的

非零平方数。

6.3 以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 为根的多项式

1. $y^3 = 2\sqrt{2}+6\sqrt{3}+9\sqrt{2}+3\sqrt{3} = 11\sqrt{2}+9\sqrt{3}$，而 $9y = 9\sqrt{2}+9\sqrt{3}$，所以 $y^3-9y = 2\sqrt{2}$。于是 $\sqrt{3} = y-\sqrt{2}$ 和 $\sqrt{6} = \sqrt{2}\sqrt{3}$ 也都是 y 的多项式。

2. 设 $x-\sqrt{2} = \sqrt[3]{3}$ 并取立方：$x^3+6x-3 = \sqrt{2}(3x^2+2)$。两边平方得 $x^6-6x^4-6x^3+12x^2-36x+1=0$。

3. 可能的有理根只有 ±1，而两者都不是根。由于没有 x^3 项，分解成两个首一（monic）二次式时必定形如 $(x^2+ax+b)(x^2-ax+c)$，其中 $a(c-b)=0$、$b+c-a^2=-10$ 及 $bc=1$。若 $a=0$，则 $b+c=-10$ 且 $bc=1$，在整数范围内不可能；若 $b=c=\pm1$，则 $a^2=12$ 或 8，同样不可能。所以这个四次式不可约（irreducible），而 $\sqrt{2}+\sqrt{3}$ 的次数（degree）为 4。

4. 由棣美弗（De Moivre）定理，$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$；取 $\theta = 20^\circ$，得 $\frac{1}{2} = 4c^3-3c$。候选的有理根 $\pm1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ 全都不成立。所以 $\cos 20^\circ$ 的次数为 3，但每个可作图（constructible）长度的次数都是 2 的幂，因此无法由 60° 作出 20°。

6.4 解四次方程

1. $y_1y_2+y_2y_3+y_3y_1$ 是十二项 $\alpha^2\beta\gamma$（一个根的平方乘以另外两个根）之和。而 $\left(\sum\alpha\right)\left(\sum\alpha\beta\gamma\right)$ 则是这十二项再加上 $4\alpha\beta\gamma\delta$。所以所求之和为 $(-p)(-r)-4s$。

2. 比较系数得 $a+b=1$、$a\alpha+b\beta=0$ 及 $a\alpha^2+b\beta^2=-p$，当 $\alpha\neq\beta$ 时有解，而这正是那两个条件所保证的：$p\neq0$ 使关于 t 的方程是真正的二次方程（若 $p=0$，它会退化成 $-qt=0$，只有单一个根 0），而 $q^2\neq4p^3$ 则使它的判别式（discriminant）q^2-4p^3 不为零。对于 $x^3-24x+48$：$p=8$，$q=48$，而 $8t^2-48t+64=0$ 给出 $\alpha=2$，$\beta=4$。于是 $\left(\frac{x-2}{x-4}\right)^3 = -\frac{b}{a} = \frac{\alpha}{\beta} = \frac{1}{2}$，所以 $x-2 = 2^{-1/3}(x-4)$，整理后即得题中给出的根，$x\approx-5.6946$。

3. 预解三次式（resolvent cubic）为 $y^3-7y^2+16y-12 = (y-3)(y-2)^2$。由根 $y=3$ 得出 $(x^2-2x+1)(x^2-2x+2)$，所以各根为 1（二重根）和 $1\pm\mathrm{i}$。

4. 在每一对之内可以对换或不对换（4 种选择），两对之间也可以互换或不互换（2 种选择）：恒等置换、$(\alpha\beta)$、$(\gamma\delta)$、$(\alpha\beta)(\gamma\delta)$、$(\alpha\gamma)(\beta\delta)$、$(\alpha\delta)(\beta\gamma)$、$(\alpha\gamma\beta\delta)$ 和 $(\alpha\delta\beta\gamma)$。这与正方形的对称群（symmetry group）结构完全相同。

6.5 从公理出发的微分法

1. 常数仍然给出 0，而由规则 (i) 及归纳法（induction）可得 $\lozenge x^n = x^{n-1}\lozenge x + x\lozenge x^{n-1} = nx^n$。再由线性（linearity）得 $\lozenge\mathrm{h} = x\mathrm{h}'$。

2. $\Diamond \mathrm{f} = \frac{\mathrm{f}}{\mathrm{g}} \Diamond \mathrm{g} + \mathrm{g} \Diamond \frac{\mathrm{f}}{\mathrm{g}}$，所以 $\Diamond \frac{\mathrm{f}}{\mathrm{g}} = \frac{\mathrm{g} \Diamond \mathrm{f} - \mathrm{f} \Diamond \mathrm{g}}{\mathrm{g}^2}$。

3. 若 $\mathrm{f} = (x-a)^2 \mathrm{g}$，则 $\mathrm{f}' = (x-a)\big(2\mathrm{g} + (x-a)\mathrm{g}'\big)$。$x^n - 1$ 的重根（repeated root）必定也是 nx^{n-1} 的根，所以只能是 0；但 0 并不是 $x^n - 1$ 的根。

4. $(2+\varepsilon)^2 + 1 = 5 + 4\varepsilon$，而 $(5+4\varepsilon)^3 = 125 + 300\varepsilon$。所以 $f(2) = 125$ 及 $f'(2) = 300$；用链式法则（chain rule）则得 $3(x^2+1)^2 \cdot 2x = 3 \cdot 25 \cdot 4 = 300$。

6.6 子群的并集

1. 设 $V = \{e, a, b, c\}$：$a^2 = b^2 = c^2 = e$，而 a、b、c 之中任意两个之积都是第三个。每个元素都是自己的逆元（inverse）。在 $\{1, \mathrm{i}, -1, -\mathrm{i}\}$ 中，i 的逆元是 $-\mathrm{i}$，所以这两个群并不相同。

2. 假如 g 属于某个真子群（proper subgroup）H，那么 g 的每个幂也都属于它，于是 H 就是整个群。

3. 1 既不是偶数，也不是 3 的倍数。更一般地，$\mathbb{Z}$ 是循环群（cyclic group，由 1 生成），所以根据上一题，它不是任意多个真子群的并集（union）。

4. 直线 $y = mx$ 与 $y = x^2$ 只相交于 $x = 0$ 和 $x = m$ 两处，而直线 $x = 0$ 与它只相交于原点。所以 k 条直线最多只能包含 k 个形如 (t, t^2) 而 $t \neq 0$ 的点，但这样的点有无穷多个。

6.7 四元数群

1. $C \circ B = (\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i}) = D$，而 $B \circ C = (0, 1) \circ (\mathrm{i}, 0) = (0, \mathrm{i}^*) = (0, -\mathrm{i}) = H$。

2. A 的阶（order）为 1，E 的阶为 2；其余六个元素的平方都是 E，所以阶为 4。正方形的对称群有五个阶为 2 的元素（四个反射和一个半周旋转），所以这两个群并不同构（isomorphic）。

3. $\det M = z_1 z_1^* + z_2 z_2^* = |z_1|^2 + |z_2|^2$，这是四个实数平方之和。由于 $M(z)M(w)$ 是 $z \circ w$ 的矩阵，把行列式（determinant）相乘，便可把 $(a_1^2 + \cdots + a_4^2)(b_1^2 + \cdots + b_4^2)$ 写成 $|u_1|^2 + |u_2|^2$，同样是四个平方之和。

4. 各子群为 $\{A\}$、$\{A, E\}$、$\{A, E, C, G\}$、$\{A, E, B, F\}$、$\{A, E, D, H\}$ 和 Q_8。除 A 以外，每个元素都有某个幂等于 E，所以除 $\{A\}$ 以外的任何子群都包含 E。三个阶为 4 的子群合起来包含了全部八个元素。

6.8 由奇异矩阵组成的群

1. $\mathbf{M}_a \mathbf{M}_b = \mathbf{M}_{2ab}$，而 $2(2ab) = (2a)(2b)$。这个映射是一对一（one-to-one）的，并且映成（onto）全体非零实数。

2. $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$，其中 $ac \neq 0$，所以这个集合是封闭（closed）的。每个 $\begin{pmatrix} 1 & e \\ 0 & 0 \end{pmatrix}$ 都是左单位元（left identity）。但若要 $\mathbf{XE} = \mathbf{X}$，其中 $\mathbf{E} = \begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix}$，便需要 $e = 1$ 及 $f = b/a$，而后者取决于 $\mathbf{X}$：所以没有右单位元，因而没有单位元，也就不成群。

3. $\mathbf{0}$、$\mathbf{I}$，以及满足 $bc = a(1-a)$ 的矩阵 $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$（迹（trace）为 1，行列式为 0）。这些就是把平面沿一条直线的方向投影（projection）到另一条直线上的变换。

4. 所有元素均为 a 的矩阵 $\mathbf{J}_a$ 满足 $\mathbf{J}_a\mathbf{J}_b = \mathbf{J}_{nab}$。单位元是 $\mathbf{J}_{1/n}$，而 $\mathbf{J}_a$ 的逆元是 $\mathbf{J}_{1/(n^2a)}$。

Beyond STEP

STEP 是大多数中学生一生中应考过最艰深的数学考试，也是最出色的考试之一：题目简短、陌生而深刻，当中最精彩的，其实是乔装了的大学数学小品。

本书精选最有趣的 STEP 试题，由 1987 年首次开考之前的样本试卷（specimen papers），到 2025 年的试卷，并以每一道题目作为一扇门。每道题目都会仔细解答，沿途提出优秀学生会问的问题，然后带你穿过这扇门：这个想法从何而来，到了大学会演变成甚么，以及接下来该读些甚么。

本书为正在准备 STEP、有天分又有志投身数学的学生而写。他们想要的不止是模拟试卷：他们想开始像数学系本科生那样思考，并一探前方有甚么正等着自己。

- 共 13 章，涵盖纯数学（pure mathematics）、力学（mechanics）、概率（probability）与统计（statistics）
- 136 道 STEP 历届试题，每题均附引导式解答
- 每道题目背后的大学数学
- 附答案的延伸练习，以及延伸阅读

全书共 13 章，本册为第 6 章。 全书各章及所有详细解答均可免费阅读、下载及分享，网址为

beyondstep.keithmcnulty.org

文字内容已贡献予公有领域（CC0 1.0）。STEP 试题 © Cambridge University Press & Assessment。

